University of Macedonia
School of Information Sciences
Department of Applied Informatics

Algorithms and Scenarios for Efficient and Secure Big Data Delivery, Management, and Analysis over the Internet of Things

Doctoral Thesis of Andreas P. Plageras

Doctoral Thesis Committee:
Konstantinos E. Psannis, Associate Professor, University of Macedonia (Supervisor)
Petros Nikopolitidis, Associate Professor, Aristotle University of Thessaloniki
Panagiotis Papadimitriou, Associate Professor, University of Macedonia

Thessaloniki, 2022

“Algorithms and Scenarios for Efficient and Secure Big Data Delivery, Management, and Analysis over the Internet of Things”

Andreas P. Plageras

MSc in Applied Informatics, University of Macedonia, 2016
BSc in Information Technology, Computer Technology, and Engineering - University of Western Macedonia, 2013

Thesis submitted

in partial fulfillment of the requirements for the
Doctorate degree in Computer Science

Examination Committee:

_____
Konstantinos E. Psannis, Associate Professor, University of Macedonia

_____
Petros Nikopolitidis, Associate Professor, Aristotle University of Thessaloniki

_____
Panagiotis Papadimitriou, Associate Professor, University of Macedonia

_____
George Kokkonis, Assistant Professor, University of Western Macedonia

_____
George Fragkoulis, Professor, University of Western Macedonia

_____
Nikos Asimopoulos, Professor, University of Western Macedonia

_____
Michalis Dosis, Professor, University of Western Macedonia

_____
Author: Andreas P. Plageras

Thessaloniki, July 2022

Acknowledgements

I would like to express my gratitude to my supervisor, professor Dr. Konstantinos E. Psannis, for inviting me to join his team "Mobility2Net" (Mobility2Net - YouTube) at the University of Macedonia. In addition, I appreciate his unwavering support, his always comprehensive and prompt criticism, and his never-ending patience. Without his assistance and understanding, I would not have been able to finish this dissertation. He has shown me how to be an autonomous scientist while also being an active member of a research group, in addition to imparting vital academic information. During the five years of my PhD studies, we worked in perfect harmony, and his helpful advice was invaluable in conquering the numerous challenges I experienced.

My profound gratitude goes out to my friends and colleagues Dr. Christos L. Stergiou and Dr. George Kokkonis, without whom my research would not have been finished. Our collaboration was flawless, and it frequently resulted in excellent research results, which were extremely beneficial to the continuation and completion of my research. Working with them has been a real privilege. I am looking forward to working with them in the future.

My thankfulness for my family is beyond words. They showed me unconditional love, made many sacrifices, and believed in every concept I had over the years. They were always there for me, helping and supporting me throughout my studies and research.

Last but not least, I want to express my gratitude to Rea for her unwavering love and support.

Abstract

All recent technology findings could be involved and combined to strengthen and support the “Internet of Things” (IoT) sector. The novel technology of “Multi-Access Edge Computing” or “Mobile Edge Computing” (MEC) rises rapidly in the industry as well as the “Digital Twins”. MEC is the middle-layer between mobile devices and cloud, which offers scalability, reliability, security, efficient control, and storage of resources. In addition, digital twins form a communication model that will enhance the whole system by improving the latency, the overhead, and the energy consumption. The overall paper is focused on the biggest challenges that researchers in the field of IoT have to overcome in order to gain a more efficient communication environment in terms of technology integration, efficient energy, data delivery, storage spaces, security, and real-time control and analysis. First, IoT, surveillance, haptics, and other devices have been configured, installed, and programmed with suitable algorithms. Then, the databases and the broker devices have been also installed and programmed to work efficiently with the IoT devices. Moreover, a framework has been proposed in order to reduce the traffic and the latency by merging the processing of the data generated by the IoT devices at the edge of the network. Machine learning algorithms have been also tested and compared in order to make the best choice for each case. The evaluation of critical parts of the proposed IoT systems have been performed both with emulation/simulation software and in real environments with real devices. The results have shown that data delivery and offloading have been done more efficiently, the energy consumption and the processing have been improved, and the security, the complexity, the control, and the reliability have been enhanced.

Keywords

4G; 5G; Algorithms; Applications; AI; Analytics; Architectures; Big Data; Cloud Computing; Edge Computing; Energy Efficiency; Frameworks; Haptics; IoT; IPv6; Load Balancing; Machine Learning; Management; MEC; NDN; Networking; Platforms; Privacy; Protocols; Security; Sensing; Transmission; Ubiquitous Computing; WSNs;

Contents

List of Figures Page

List of Tables Page

List of Algorithms Page

Abbreviations

3D	Three Dimensional
3DES	Triple Data Encryption Standard
6LoWPAN	Ipv6 over Low power Wireless Personal Area Network
5G	Fifth Generation
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AIBSBAC	Artificial Intelligent Based Smart Building Automation Controller
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
AR	Augmented Reality
ARDC	Average Radio Duty Cycle
ARM	Advanced RISC Machines
BAS	Building Automation System
Bcrypt	Binary cryptography
BD	Big Data
BIM	Building Information Modelling
BLE	Bluetooth Low Energy
BMS	Building Management System
BTemp	Body Temperature
BV	Blood Volume
CAST	Carlisle Adams & Stafford Tvares
CC	Cloud Computing
CCyc	Clock Cycles
CD	Camera Device
CIA	Confidentiality, Integrity, Availability
CoAP	Constrained Application Protocol
CNNs	Convolutional Neural Networks
CPU	Central Processing Unit
CS	Cloud Server
CSRF	Cross-Site Request Forgery
Curr	Current
D2D	Device to Device
DCPS	Data Centric Publish/Subscribe
DDS	Data Distribution Service
DES	Data Encryption Standard
DHT	Digital Humidity and Temperature
DDoS	Distributed Denial of Service
DDSI	DataDistribution Service Interoperability
DLRL	Data Local Reconstruction Layer
DL	Deep Learning
DoS	Denial of Service
DM payloads	Device Management
DNNs	Deep Neural Networks
DNS	Domain Name Server
DOM	Document Object Model
DRL	Deep Reinforcement Learning
DSA	Digital Signature Algorithm
DTLS	Datagram Transport Layer Security

DTNs	Delay Tolerant Networks
EC	Edge Computing
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDGE	Enhanced Data rates for Global Evolution
ElecVol	Electricity Volume
EO	Edge Orchestrator
ETX	Estimated Time of transmissions
EU	European Union
EV	Energest Value
EXI	
FBMC	Filtered Multi-tone mode of filter bank MultiCarrier
FL	Federated Learning
FRI	Fuzzy Rule Interpolation
Gbps	Gigabits per second
GDPR	General Data Protection Regulation
GFDM	Generalized Frequency Division Multiplexing
GHz	Giga Hertz
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GUI	Graphical User Interface
HDFS	Hadoop Distributed File System
HR	Heart Rate
HSPA	High Speed Packet data Access
HVAC	
HTTP	HyperText Transfer Protocol
IaaS	Infrastructure as a Service
IB	Intelligent Building
ID	Identification – Identity
IDEA	
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineering
IoT	Internet of Things
IIoT	Industrial Internet of Things
IioTaaS	Industrial Internet of Things as a Service
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	International Safety Management
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
JTC	Joint Technical Committee
Kbps	Kilobits per second
LabVIEW	Laboratory Virtual Instrument Engineering Workbench
LC	Least Connections
LINP	Logically Isolated Network Partition
LLN	Low power and Lossy Networks
LNM	Localization Method
LPM	Low Power Mode

LoRaWAN	Long Range Wide Area Network
LS-SVM	Least Square Support Vector Machine
LTE	Long-Term Evolution
LwM2M	Lightweight M2M standard
M2M	Machine to Machine
MAC	Media Access Control
M.A.C.	Message Authentication Codes
Mbps	Megabits per second
MCC	Mobile Cloud Computing
MDA	Model Driven Architecture
MEC	Multi-access Edge Computing or Mobile Edge Computing
MHz	Mega Hertz
ML	Machine Learning
MPHF	Minimal Perfect Hash Table – Function
MQTT	Message Queuing Telemetry Protocol
MQTT-SN or S	Message Queuing Telemetry Protocol Sensor Network
MR	Mixed Reality
MTConnect	Manufacturing Technical Standard
MVC	Model View Controller
NAMRTP	Network Adaptive Multi-sensory Real-time Transmission Protocol
NDN	Named Data Networking
NFC	Near Field Communication
NoSQL	Non-relational Structured Query Language
NIDD	Non IP Data Delivery
OFDM	Orthogonal Frequency Division Multiplexing
OPC UA	Open Platform Communication Unified Architecture
OS	Operating System
OSCORE	Object Security for Constrained RESTful Environments
OSI	Open Systems Interconnection
OWL	Ontology Language
P2P	Peer to Peer
PaaS	Platform as a Service
PCAP	Packet Capture
PCon	Power Consumption
PDA	Personal Digital Assistant
PDR	Packet Delivery Ratio
PHP	Hypertext Preprocessor
PL	Packet Loss
QL	Query Learning
QoS	Quality of Service
RAM	Random Access Memory
RAN	Radio Access Network
RDF	Resource Description Framework
REST	REpresentational State Transfer
RF	Radio Frequency
RL	Reinforcement Learning
ROM	Read Only Memory
RPL	Routing Protocol for Low power and lossy networks
RR	Round Robin

RSA	Rivest – Shamir – Adleman
RSS	Residual Sum of Squares
RTPS	Real-Time Publish-Subscribe
RTsec	Timer in seconds
RX	Receive Transmission
SaaS	Software as a Service
SASL	Simple Authentication and Security Layer
SB	Smart Building
SC	Skin Conductance
SCTP	Stream Control Transmission Protocol
SFP	Science Fiction Prototyping
SH	Smart Home
SHA-2	Secure Hash Algorithm 2
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SRP	Secure Remote Password
SSL	Secure Socket Layer
SQL	Structured Query Language
T	period
TCP	Transmission Control Protocol
TDR	Total Data Received
TDS	Total Data Sent
TEA	Tiny Encryption Algorithm
Tint	Time Interval
TLS	Transport Layer Security
Ton	Time on
TTL	Time To Live
TX	Transmit Transmission
VR	Virtual Reality
UDP	User Datagram Protocol
UFMC	Universal Filtered MultiCarrier
UHF	Ultra-High Frequency
UMTS	Universal Mobile Telecommunications System
UPS	Universal Power Supply
WBAN	Wireless Body Area Network
Wi-Fi	Wireless Fidelity
WLC	Weighted Least Connections
WRR	Weighted Round Robin
WSN	Wireless Sensor Network
XML	eXtensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol
XOR	eXclusive OR

Chapter 1

Introduction

The first automation (non-electrical) mechanisms were invented in 270-300 BC. Since then, some "timestamps" in history can be observed and have been presented in figure 1 below. The first one is back in 1968 when the "Microcomputers" and "Microcontrollers" (transistor-transistor logic (TTL)) were invented. The microcomputers are still widely used in the present day in conjunction with the second timestamp which is back in 1969 when the Internet was invented. The third one is the mobility and the "Cellular Networks". The fourth one is at present time with the invention of technologies such as the "Internet of Things" (IoT), the "Big Data" (BD), the "Wireless Communications", the "Convolutional and Deep Neural Networks" (CNNs and DNNs), the "Cloud & Edge Computing" (CC and EC) with their services, the web applications, the "Mobile Cloud Computing" (MCC), the "Mobile Edge Computing" (MEC), the IoT applications, the "Artificial Intelligence" (AI), the "Robotics", the "Haptics", and the "Mixed Reality" (MR), which is a mix of "Virtual Reality" (VR) and "Augmented Reality" (AR), all under the umbrella of the IoT. All the aforementioned technologies have been defined in the next chapter.

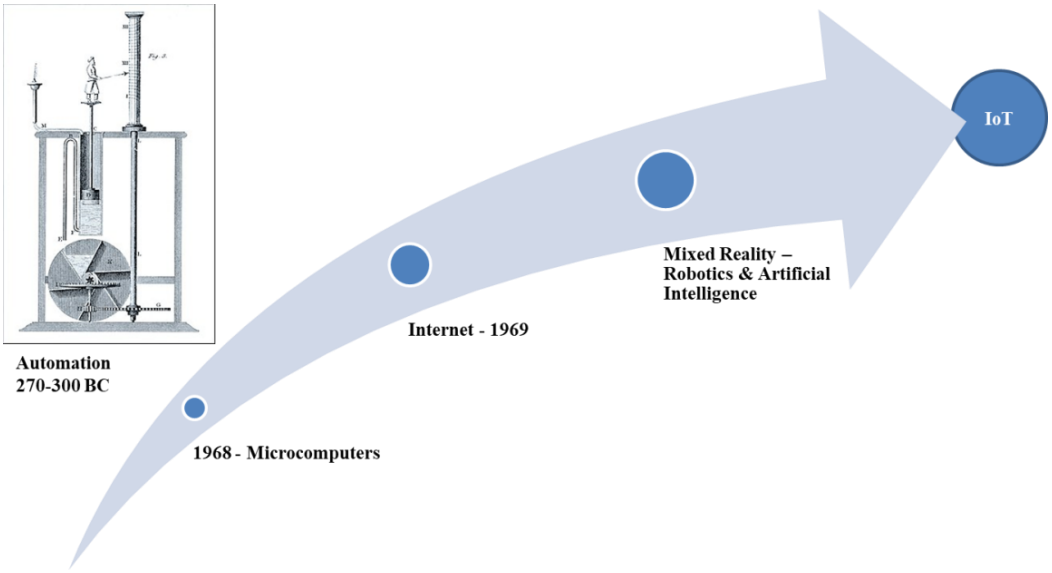


Figure 1. Electronic and network technologies revolution.

IoT consists of all physical things in our everyday life that are enriched with computing, sensing, and communication capabilities (via the internet). These autonomous things, namely IoT devices, produce a very big amount of inappropriate data, the BD. With "Machine Learning" (ML) algorithms and suitable software tools these irrelevant data can be managed, so that knowledge can be extracted and delivered. Knowledge is a term used to describe the information mined out of these data. The

destination is a software environment that is responsible for the analysis and presentation of BD.

According to surveys, the emergence of new technologies and the IoT has shown explosive growth in data. A huge number of networked devices (sensors, actuators, etc.) around the world collect different types of data (environmental, geographical, accounting, etc.). Then, the IoT devices transmit the collected data so that they can be stored, processed, and analyzed.

Also, studies have shown that by 2030 approximately more than one trillion sensors will be connected, which will collect and transfer large amounts of data. Therefore, there is an urgent need for the adoption of applications based on big data and IoT. These technologies are interdependent and should be developed jointly. Specifically, on the one hand, there has been the wide spread of IoT, leading to the increase of data, thus providing the opportunity for application and development of BD. On the other hand, the implementation of IoT-BD accelerates research advances and business models of IoT (Min Chen et al., 2014).

In other words, people in their daily life come in touch with countless devices and other technological advances. These devices are connected and form a network, which leads us to the IoT. This new technological trend is accompanied by countless development and improvement expectations in all areas (healthcare, education, industry, transportation, buildings, etc.). Also, this new technological trend comes along with concerns about security and the violation of privacy (Andreas P. Plageras et al., 2016).

The general purpose of this dissertation is to make these advances much more accessible, much faster, more efficient, and of course safer for everyone and everywhere, even in the poorest and farthest destinations. In this way, with sensors, actuators, cameras, haptic devices, and other components everyone can monitor, manage, analyze, secure, and gain all the benefits of the IoT technology.

The main purpose of this dissertation is to create and propose, after study and experimentation, suitable algorithms, solutions, and scenarios for dealing with the efficient delivery of BD (in and out of a network, the internet, and cloud), the management, the analysis, the energy efficiency, and the security of the IoT-BD.

After exhaustive research in the sectors of healthcare, education, transportation, industrial, and living in a smart city in general, it can be said that this dissertation contributes by enriching the research areas it covers, with new and innovative ideas and applications in terms of data transmission, energy efficiency, and security.

1.1 Open Issues in the Field

All these advances aforementioned came together with new issues in the IoT era. Some of them have been listed below.

Data standards are used for collecting, transmitting, exchanging, sharing, handling, storing, securing, printing, and retrieving data related to the needs of each smart system. So, these standards surround protocols, methods, specifications, and

terminologies. Different standards behave servilely to different sectors by delivering efficiently critical information between systems. So, the selection of the appropriate standard and protocol is a challenge since it is contingent on the IoT system, its nature, and its demands.

Another challenge to overcome is the interoperability of the remotely managed smart IoT system. Due to this need, public communication networks with private communication lines have been widely used. To interconnect these networks over a common medium, it is indispensable to develop standards that determine interfaces between clients and servers in a network.

Furthermore, the increasing number of network-based applications that support the IoT networks should be divided into liturgical pieces. The protocols enable communications with the relative layers and all together compose the network architecture.

Nevertheless, international standards are used for the protection of sensitive and personal data. Such standards are used by governments to build legislation to protect and improve their communities. So, all data can be divided into two groups, structured data, and unstructured data. On the one hand, the structured data carry personal information such as name, surname, birthdate, test results, and so on. These data comply with standards and they can be transferred without any difficulty. On the other hand, unstructured data do not comply with standards and can be data relevant to email messages, multimedia such as records, audio, images, animations, and so on.

All IoT devices are connected to the Internet and are controlled and monitored remotely via applications. In most cases, these devices have constrained resources and thus, there is a need for novel network protocols and technologies that will ensure these objects. Due to this need, various protocols have been proposed for every single tier of the IoT communication model.

The rapid growth of data, due to the huge number of networked sensors around the world that collect, transmit, store, and process different types of data, bring enormous challenges for the acquisition, the storage, the management, and the data analysis. Min Chen et al. discussed in their research some of the key challenges. (Min Chen et al., 2014)

All these, concerns:

- the representation of the health data, to create more comprehensible health data for computational analysis and interpretation of the user,
- the management of data life cycle with the development of mechanisms which will be the selection of data that will be stored and those that will be rejected,
- the reduction of the redundancy which exists in the health data and the compression of these data,
- the detailed mechanisms,
- the storage capacity and the storage media,
- the confidentiality of BD,
- the management of energy,

- the scalability and consumability, as well as, analytical systems and analytical algorithms should be adapted to different and more complex data sets, and
- the collaboration between scientists from different disciplines and the development of architectures of large e-health data networks to help these scientists.

Researchers have also to overcome fundamental problems of BD (definitions and models), the standardization of BD, and the development of computational methods for BD.

Continuing with the challenges, there have to be mentioned those that deal with the analysis of BD (BD analytics). Specifically, researchers talk about the need that exists for speed and quality of data, and the need for larger storage spaces, such as the 'cloud'. CC technology is considered the future technology that will provide storage spaces and mechanisms for data analysis. Also, researchers will need experts on the subject to educate new entrants in this field, because BD is a new research field. The integration of different data types is also a challenge (Sunita and Yugchhaya, 2016).

In addition, researchers discuss open issues and challenges of mining large data. One of the important issues is the protection of personal data. To produce information by extracting data requires personal information. Privacy is lost as well, through social media where an individual's data can be extracted. Thus, researchers and scientists should consider in-depth and create new tools to address these issues. Also, another important issue mentioned in this research is the user interaction by using feedback/guidance allowed during data mining, to enable the user to visualize, interpret and evaluate the results, whether they are finished or intermediate (Abhinav Kathuria, 2016).

The "Industrial Internet of Things" (IIoT) is a smart network of machines and devices interacting to improve the performance of each industrial process (Hsiao and Lee, 2021). IIoT means that there is a need for more efficient "Device-to-Device" (D2D) connectivity and communication, more time savings, more efficient optimization, a more secured environment, and more. In IIoT there are many different standards, protocols, and technologies that deal with the different devices and systems. The connections are both wired and wireless (M. Mahalingam, 2021).

A challenge that arises in the IIoT systems is the data collection and transmission which have to be done with limited energy (Xiaolin Fang et al., 2018). Moreover, the integration and interoperability issues have to be solved (Hsiao and Lee, 2021). Another relevant issue is the connectivity between devices (M. Mahalingam, 2021). Different IoT devices use different protocols to communicate since each device produces different kinds of data. The challenges and issues that have been considered key elements to meet the sustainability needs are not limited to the availability, the scalability, the reliability, the response time, the power consumption, the security, and the cost.

Researchers claim that since the IoT devices have reached 50 billion and the data generated by them 500 zettabytes, it has been emerging to develop novel networking, storage, and energy-constrained solutions.

Major problems are related to security due to the sensitivity of the personal data or data that will lead to economic, and political scandals or even can cause life loss. Some of the security problems are the confidentiality of BD, the availability of BD, and the integrity of BD, or as they have been called the "*CIA triad*". But it is not required for IoT to lift itself the burden of data security and the personal life of users.

In table 1 below, some of the most crucial threats that have been studied by the scientific community in the field can be observed. These threats can be considered the most important parts that have to be deployed properly for every system. Authentication for example is a basic and the first component that deals with the safe access of individuals. The encryption of the data to be sent safely must be an integral part of the communication system too. The location is for the safety of individuals and buildings since they are moving due to mobility. But these mobile users have been vulnerable due to the constrained energy and the low complexity algorithms and protocols that have been used in such environments.

Table 1. Crucial Threats in IoT Environments.

Threats	**Definition**
Authentication	New security access models have to be implemented to overcome the constrained energy and processing capabilities of IoT devices.
Encryption	Information exchange under strict rules.
Location	Monitored and tracked
Insecure Protocols	Protocols must be compressed in such a way to provide the appropriate levels of security.
Mobility	The mobility of the devices, the constrained energy, and the computational resources are critical issues.
Identification	Use specific ids to identify every different device.

1.2 Problems Definition

IoT is a novel technology that has gained great attention in every sector worldwide. As it can be said after experimentation and studies IoT has a purpose, to connect everything (electronic devices, data, Internet, applications, platforms, people, etc.) to gain the most of this technology. Specifically, the devices are connected producing data over time. The connected devices form "Wireless Sensor Networks" (WSNs) that are equipped with wireless and other communication capabilities. Some data should be handled in real-time because of their critical subsistence. There comes the technology of "Edge Computing". Others cannot be handled, due to the complex mechanisms and applications that are required for their management, storage, processing, transfer, and analysis, so they are sent up to the clouds ("Cloud Computing").

Most of the data have to be compared or grouped in order to take serious decisions or decisions that need speed (e.g., emergencies). Speed means quick data transfer and management. For such purposes has been widely used data learning technologies. Such technologies are "Machine Learning", the "Query Learning", the "Deep Learning", the "Reinforcement Learning", the "Deep Reinforcement Learning", the "Federated Learning", and more. Some of these technologies have been used for

real-time handling of “Big Data” and some others for the construction of decision-making systems.

Moreover, many new technologies, such as “Haptics”, “Robotics”, “Virtual Reality”, “Augmented Reality”, and “Surveillance”, have been adopted in the IoT era. These technologies can change from the ground up serious problems and situations that could not be solved before. These issues are related to healthcare, education, communication, living, transportation, safety, energy, and other critical issues.

But to do so, citizens must be motivated to adopt these advances in their everyday life. In addition, the technology must be handled in a way that takes into consideration human rights and does not affect negatively their everyday life. Despite, a big percentage of the global population that is not ready for such a step forward, the scientific community should give all appropriate attention to the stimulation of the crowd.

1.3 Motivation and Scope

The general purpose of this dissertation is to make the aforementioned advances and technologies much more accessible and much faster for everyone and everywhere there is a connection to the Internet. In this way, with sensors, actuators, cameras, and other components everyone can monitor, manage, analyze, and gain all the benefits of the “Internet of Things” (IoT) technology.

The main purpose of this dissertation is to develop and propose, after study and experimentation, novel ideas, systems, suitable algorithms, mechanisms, solutions/scenarios, and tools for dealing with the efficient delivery of the BD (in and out of a network, over the internet and beyond this, to the CC), the management, the analysis, the energy efficiency, and the security of the IoT-BD. Due to these technological advances, the quality and safety of living will be improved.

1.4 Thesis Contribution

The results of this dissertation, contribute to the theoretical and the applied scientific knowledge.

From the perspective of theoretical knowledge, there have been proposed novel frameworks and architectures that can integrate any data transport protocol for real-time communications over the Internet. These frameworks, architectures, and protocols used, will adapt to different kinds of sensors in the general scientific field of “Wireless Sensor Networks” (WSNs). Moreover, energy consumption has been measured and taken into consideration since it plays a vital role in the efficiency of IoT systems and the ability to use more complex security algorithms. So, this dissertation has also proposed, after study and exhaustive research, the best way to protect the transmitted and stored “Big Data” (BD). Furthermore, the “Machine Learning" (ML) algorithms have been compared and tested in a proposed IoT system.

From the perspective of applied scientific knowledge, particular emphasis has been given to the proposed IoT communication model. The three layers of this model

have been implemented, tested, and evaluated in different projects, with different tools, and for different situations. Various IoT devices, surveillance devices, haptic devices, broker devices, and databases have been installed and programmed. Last but not least, application development and systems programming have been well researched. Novel frameworks, applications, and algorithms have been integrated to support IoT technology.

1.5 Thesis Outline

This chapter has discussed the motivation, the scope, and the main objectives of our work and outlined the major contributions of this thesis. The remaining chapters are structured as follows:

- Chapter 2 presents the Internet of Things technology.
- Chapter 3 discusses Big Data and Data Learning technologies.
- Chapter 4 deals with communication and networking in IoT.
- Chapter 5 presents the Edge Computing technology.
- Chapter 6 discusses Cloud Computing technology.
- Chapter 7 presents the Artificial Intelligence technology.
- Chapter 8 deals with frameworks, platforms, and applications.
- Chapter 9 discusses Energy Efficiency in IoT.
- Chapter 10 deals with the Security and Privacy in IoT.
- Chapter 11 lists the proposed convergence of technologies and solutions.
- Chapter 12 presents the testing, the evaluation, and the experimental results.
- Chapter 13 presents the contribution and the novelty of the dissertation.
- Chapter 14 concludes the dissertation.
- Chapter 15 lists some future work and future directions.

1.6 Publications

All the important research findings of this dissertation have been published in peer-reviewed journals and conference papers. All papers underwent extensive reviewing processes before the actual publication to the scientific community. The complete list of publications has been presented below.

International Journals Under Review:

1. **Andreas P. Plageras**, Christos Stergiou, Vasilis Memos, George Kokkonis, and Kostas E. Psannis, “Haptic Data Representation and Device Manipulation for IoT Applications”, 2022. (To be submitted)
2. **Andreas P. Plageras**, Kostas E. Psannis, and Zhihan Lv, “Secure Edge Communications over the IoT”. (To be submitted)
3. **Andreas P. Plageras** and Kostas E. Psannis, “Digital Twins and Multi-Access Edge Computing (MEC) for Industrial IoT”, Virtual Reality & Intelligent Hardware, Special Issue on Digital Twins, Submitted 2022. (Under Review)

International Journals Publications

1. **A. P. Plageras** and K.E. Psannis, IoT-based health and emotion care system, Elsevier, *ICT Express* (2022), Impact Factor: 4.317. DOI: https://doi.org/10.1016/j.icte.2022.03.008.
2. **A. P. Plageras**, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, "Efficient IoT-based sensor Big Data collection-processing and analysis in Smart Buildings", Future Generation Computer Systems, vol. 82, pp. 349-357, May 2018. Impact Factor: 7.187. DOI: https://doi.org/10.1016/j.future.2017.09.082

International Conferences Publications

1. **Andreas P. Plageras**, Kostas E. Psannis, George Kokkonis, and Yutaka Ishibashi, "Efficient Big Data Delivery over IoT networks", IEEE, WSCE 2021, The 4th World Symposium on Communication Engineering, 25-28/11/2021.
2. **A. P. Plageras**, C. L. Stergiou, K. E. Psannis, "Internet of Things for Healthcare: Challenges & Perspectives", in Proceedings of New Technologies in Health: Medical, Legal & Ethical Issues, 21-22 November 2019, Thessaloniki, Greece.
3. **Andreas P. Plageras**, Kostas E. Psannis, C. Stergiou, G. Kokkonis, Y. Ishibashi, "Solutions for interconnectivity and security in smart buildings", 15th International Conference on Industrial Informatics (INDIN`2017), Emden, Germany, 24-26, July 2017. DOI: 10.1109/INDIN.2017.8104766. https://ieeexplore.ieee.org/document/8104766/
4. **Andreas P. Plageras**, K. E. Psannis, "Algorithms for Big Data Delivery over the Internet of Things", in Proceedings of 19th IEEE Conference on Business Informatics 2017 (CBI`2017), Doctoral Consortium, 24-26 July 2017, Thessaloniki, Greece. DOI: 10.1109/CBI.2017.27. https://ieeexplore.ieee.org/document/8010723/
5. **Andreas P. Plageras**, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, Byung-Gyu Kim, Brij Gupta, "Efficient Large-Scale Medical Data (eHealth Big Data) Analytics in Internet of Things", in Proceedings of 19th IEEE International Conference on Business Informatics (CBI`17), International Workshop on the Internet of Things and Smart Services (ITSS'2017), 24-26 July 2017, Thessaloniki, Greece. DOI: 10.1109/CBI.2017.3. https://ieeexplore.ieee.org/document/8012935/
6. **Andreas P. Plageras**, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, "IoT-based Surveillance System for Ubiquitous Healthcare", 42nd Annual Conference of the IEEE Industrial Electronics Society (IECON`2016), Piazza Adua, 1 - Firenze (Florence), Italy October 24-27, 2016. DOI: 10.1109/IECON.2016.7793281.

Peer-reviewed papers related to the main scope of the dissertation but not part of the basic research of it are listed below. Full papers are represented in the Appendix of this dissertation.

Book Chapters

1. C. Stergiou, **A. P. Plageras**, K. E. Psannis, B. B. Gupta, "Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network", Springer, Handbook of Computer Networks and Cyber Security: Principles and Paradigms, Multimedia Systems and Applications, in Press, 2019.
   Link:
   https://www.researchgate.net/publication/327386664_Secure_Machine_Learning_scenario_from_Big_Data_in_Cloud_Computing_via_Internet_of_Things_network

International Journals

1. Georgios M. Minopoulos, Vasileios A. Memos, Christos L. Stergiou, Konstantinos D. Stergiou, **Andreas P. Plageras**, Maria P. Koidou, Konstantinos E. Psannis, "Exploitation of Emerging Technologies and Advanced Networks for a Smart Healthcare System", Applied Sciences Journal, Submitted on 15/04/2022. Impact Factor: 2.679. (Accepted)
2. C. Stergiou, K. E. Psannis, **A. P. Plageras**, Y. Ishibashi, B.-G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking", Journal of Multimedia Information Systems, vol. 5, no. 1, pp. 1-10, March 2018. DOI: http://dx.doi.org/10.9717/JMIS.2018.5.1.27

International Conferences

1. C. Stergiou, **A. P. Plageras**, K. E. Psannis, T. Xifilidis, G. Kokkonis, S. Kontogiannis, K. Tsarava, A. Sapountzi, "Proposed High Level Architecture of a Smart Interconnected Interactive Classroom", in Proceedings of IEEE conference SEEDA-CECNSM 2018, 22-24 September 2018, Kastoria, Greece. [DOI: 10.23919/SEEDA-CECNSM.2018.8544922].
2. C. Stergiou, K. E. Psannis, **A. P. Plageras**, T. Xifilidis, B. B. Gupta, "Security and Privacy of Big Data for Social Networking Services in Cloud", in Proceedings of IEEE Conference on Computer Communications (IEEE INFOCOM 2018), Workshop on CCSNA: Cloud Computing Systems, Networks, and Applications, 15-20 April 2018, Honolulu, HI, USA.
3. C. Stergiou, K. E. Psannis, **A. P. Plageras**, G. Kokkonis, Y. Ishibashi, "Architecture for Security in IoT Environments", in Proceedings of 26th IEEE International Symposium on Industrial Electronics (ISIE`2017), 19-21 June 2017, Edinburgh, Scotland, UK. DOI: 10.1109/ISIE.2017.8001447. https://ieeexplore.ieee.org/document/8001447/

Chapter 2

Internet of Things

2.1 Overview

In recent years, with the everyday advances and continuous research in the field of internet, wireless communications, and IoT-applications development, new technologies arise. Such technologies are wireless connectivity, cellular and deep neural networks, mobile and web applications, cloud and edge computing, with their services and not limited to these, all under the umbrella of the "Internet of Things" (IoT). The novel technology of IoT could offer new solutions and new properties in many scientific fields such as healthcare. (D. Tomtsis et al., 2015; Tuan Nguyen Gia et al., 2015)

IoT consists of all physical things in our everyday life that are enriched with computing, sensing, and communication capabilities (via the internet). These autonomous things, namely IoT devices, produce a very big amount of inappropriate data. With algorithms and suitable software tools, these irrelevant data can be managed so that knowledge is extracted. Knowledge is a term used to describe the information mined out of these data. In figure 2 below, the aforementioned have been presented.

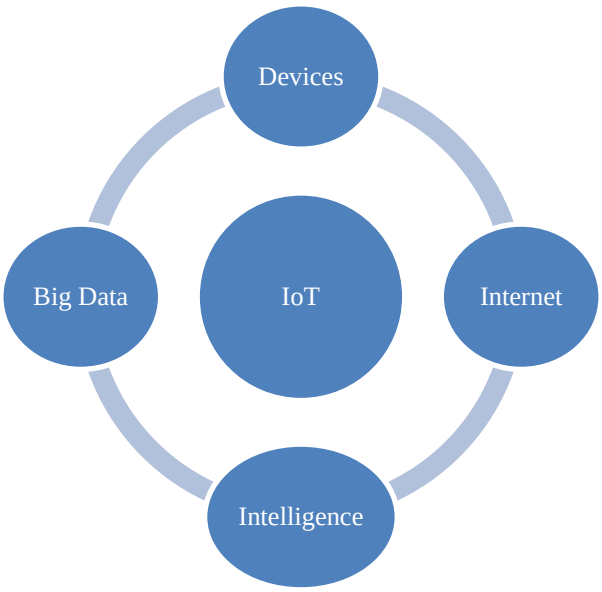


Figure 2. Internet of Things Overview.

Specifically, all the digital objects can communicate with each other connected in a network to exchange and transmit various types of data. Automatically an "Identification" (ID) which is called an "Internet Protocol" (IP) address is assigned to every object which is connected to a network. Particularly, in recent years a new version of the Internet Protocol has been developed so that every device in the world can connect to the internet and communicate (C. Stergiou et al., 2017a; A. P. Plageras et al., 2018).

2.2 IoT Communication Model

The IoT communication model that was first adapted has seven layers as shown on the right side of figure 3 below. In the following figure, a comparison between the IoT communication model, the "Open Systems Interconnection" (OSI) model, and the "Transmission Control Protocol/Internet Protocol" (TCP/IP) model can be observed.

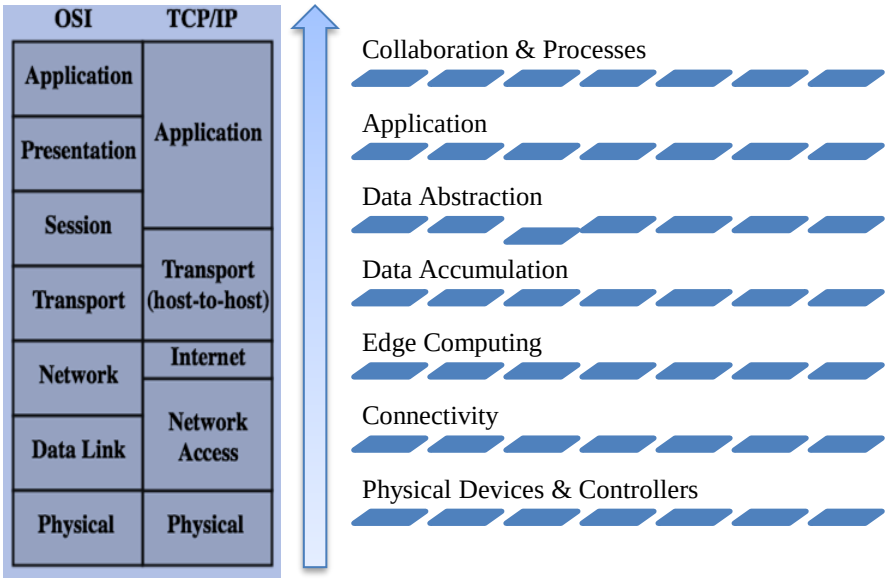


Figure 3. Internet of Things communication model.

The first layer of the OSI and TCP communication model is the physical layer, where the IoT devices and controllers belong. The second layer is the connectivity layer where all these devices and controllers connect in a way and topology so that they produce valuable information. The third layer is the edge computing layer where the valuable information should be transformed into valuable actions or transferred for further analysis over the Internet to the cloud. The fourth layer namely data accumulation is a component layer that works as a transmission hub between modeled data and query-based data consumption. In this layer, it is defined the relevance of the data and the place to be stored. The fifth layer is the data abstraction layer, which reduces the differences between what is needed and the original data generated form. The sixth layer is the application layer where data can be manipulated and accessed by any type of user. In this layer, the application interacts with the interface directly providing common services. The seventh layer is the collaboration and processing layer supports the communication with responses and actions that should be taken against the data provided.

In this dissertation and in conjunction with the most recent advances in the IoT era, a new communication model has been demonstrated. This communication model has three layers, namely the "Physical-Abstraction" layer, the "Networking-Transportation" layer, and the "Application-Presentation" layer. This model architecture can be observed in the following figure 4 below.

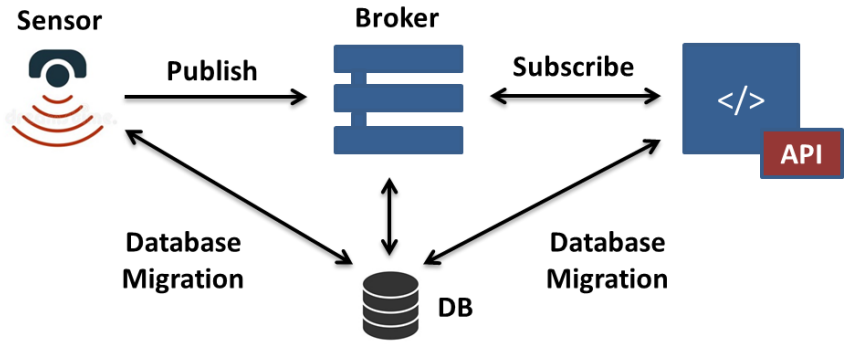


Figure 4. Proposed IoT communication model.

The first layer of the proposed communication model in this dissertation has gotten its name from the IoT devices that are inter-connected in a way and topology so that they can produce data every second efficiently. These data are useless until suitable algorithms are developed and thus, knowledge is mined out of them. These algorithms will be integrated into the code file for each sensing device. This file is stored on the server-side and includes the database connection script, the device set-up script, and the efficient algorithm. The algorithm is an efficient loop that is different for every sensor and was made to fulfill the relevant needs. For example, a body temperature sensor will update the database field that holds the value of the temperature, only when a specific change in the temperature is detected. The code is uploaded to a microcontroller such as Arduino via the Sketch application.

The second layer, which can be named the middleware, consists of a database and a broker. The local database has a table with the appropriate columns and fields to store the collected values of each device. This table was migrated by the framework. The table will work in conjunction with the mining algorithm so that the fields are updated with the new values in real-time via the broker.

The broker is software running on a device. It eliminates security issues in connections and vulnerabilities. It provides scalability from a single device to thousands of devices and manages all client connection states. Two devices can be connected and exchange messages (peer-to-peer). This is done by sending a message to the broker and then the broker forwards it to any device as a copy. This is namely the publish/subscribe model and is presented in the following figure 5.

This model is efficient and provides safety in the communications of devices and data exchange. The publisher, which can be any IoT device, transmits the data to the broker under a specified “topic”. Then the broker forwards this topic to any subscriber device that requests the specific topic. For example, in our case, the temperature sensor publishes the temperature to the broker device under the topic “temp”. The specific topic that holds the data for the temperature will be available to any subscriber that asks for the temp topic. In figure 5 below, each publisher is a different device/sensor that could be added to the system and publish a unique topic and each subscriber is the device that requests the specific topic.

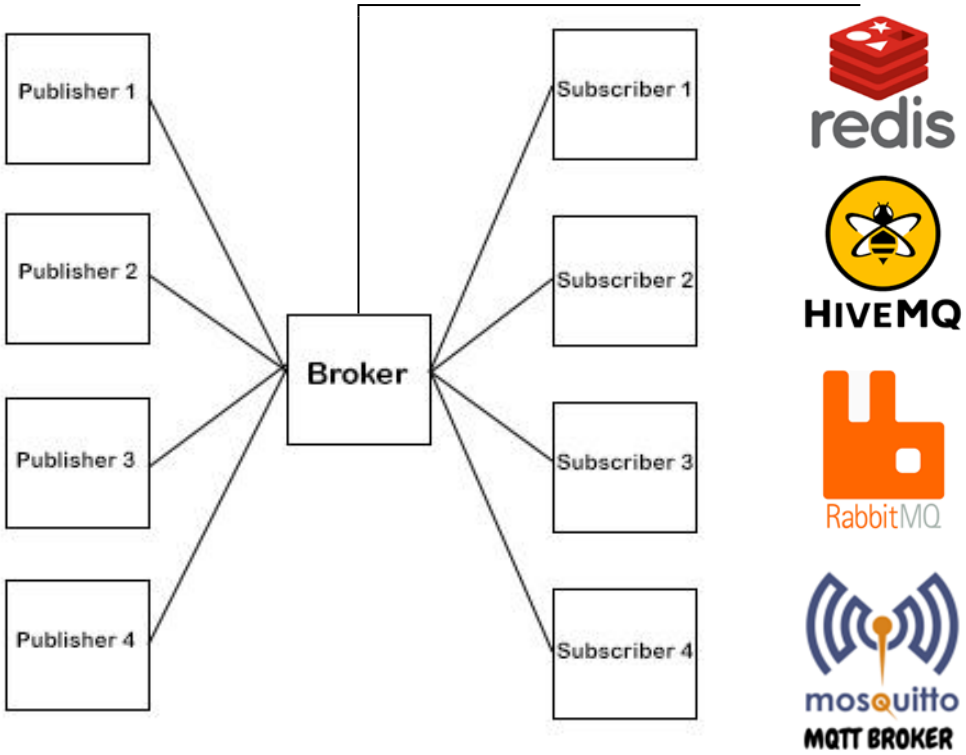


Figure 5. Publish/Subscribe communication model.

So, the broker will be responsible for the transmission of the information stored in the database to the API (Application Programming Interface) in real-time. The broker is also responsible for the transmission of the data collected to a cloud server for further analysis and complex monitoring.

In this layer, as a database and cache storage, have been used and tested the well-known MySQL database system and open-source key-value storage called Redis.

The Redis has the ability to store some data inside a key. These data are namely "a value". If the key is acquainted then the data stored in that key can be retrieved. So, the Redis database acts as a broker. This database provides also high availability and automatic partitioning.

Also, to fill up the database with fake data and test the framework a process called Seeder was used.

So, the third layer (application layer) is where the Laravel PHP framework has been used. This framework provides the DOM (Document Object Model) of the API. In simple words, it contains a structure for efficient application development and it is based on the MVC (Model-View-Controller) architecture.

2.3 Related Work

To begin with relative research in the field (Zainab H. Ali, 2020), researchers have presented a framework that makes use of different metrics in order to measure the "Quality of Service" (QoS) and achieve a sustainable "Internet of Things" (IoT) scenario. Researchers claim that since the IoT devices have reached 50 billion and the data generated by them 500 zettabytes, it has been emerging to develop novel

networking solutions. Sustainable IoT applications, challenges, and issues have also been studied and shown in this research. The challenges and issues that have been considered key elements to meet the sustainability needs are not limited to the availability, the scalability, the reliability, the response time, the power consumption, the security, and the cost. Furthermore, according to the current trends and research, another technology that has been developed jointly with the IoT is the "Cloud Computing" (CC) which offers great opportunities in terms of service management and sustainability.

Jordi Mongay Batalla et al. proposed and implemented a novel architecture for the IoT. This architecture has been based on the addressing of every object and service with identities (IDs) that correspond to their location. Every object and service form a network node since the architecture has been integrated into the network layer. So, researchers have been focused on measuring units and mechanisms of the ID of a network node. After a detailed description of the procedures of registration, promotion, and analysis, researchers have arrived at the point of the system's implementation, where after testing in Linux routers it has been concluded that the performance of the proposed system is better than previous ones. (Batalla and Krawiee, 2014)

Hui Zhou et al. have made a table of the typical QoS requirements of different kinds of devices in the smart industry. Except for the non-critical data produced by sensors and tracking devices which need low latency and low data rates (Kbps), there are many critical data produced by devices that need even lower latency, higher data rates (Mbps), and of course priority instead of the non-critical data. (Hui Zhou et al., 2021)

In the following subsections (2.3.1 – 2.3.3) related works have been presented for the most critical sectors, which have been highlighted during the research.

2.3.1 Smart Cities

Hatem Ben Sta et al. addressed the problem of imperfection in smart city-data. Also, the authors focus on the management of these not-perfect data and additionally create an evidential database by using the evidence theory in order to improve the efficiency of the smart city. A special case of modeling imperfect data in the healthcare sector is also presented in this article. Finally, a database that includes both imperfect and perfect data was built up and the various imperfect aspects, in this database are expressed by the theory of beliefs and presented in this paper. (Hatem Ben Sta, 2017)

Other authors have presented a novel approach for a research design that is based on the relationship between the components of a smart city. These components are namely, the intelligent buildings and the intelligent users. The authors also use low-cost equipment such as the Raspberry Pi, the Edison, the Arduino, and various sensors. The citizens' data and the buildings' data collected from smart mobile devices and sensors respectively, can be managed and analyzed so that they can make out more efficient cities. (L. Berntzen et al., 2016)

K. Lin, et al. proposed a localization method for pedestrians, namely the "Localization Method" (LNM). This method builds a fingerprint database with the use of the received signal strength from the neighbor. It also espouses Markov's model for predicting the position of pedestrians. Moreover, further analysis of the un-predicted signal variance is done using the history. The results are magnificent since after experimentation the proposed scheme seems to be better than others compared, even if heterogeneity problems and Wi-Fi signal variances exist. (K. Lin et al., 2016)

2.3.2 Smart Buildings

Y. Sun et al. in order to address the issues of Smart Building construction build an efficient rule engine. Specifically, it has been designed an atomic event extraction module for extracting atomic events from messages, and then build a β-network with the aim to acquire the atomic conditions for parsing the atomic trigger events. Additionally, the authors have constructed the "Minimal Perfect Hash Table" (MPHF), which can filter the majority of the unused atomic event with O(1) item overhead, by taking the atomic trigger events as the key set of MPHF. Furthermore, there is also proposed a rule engine adaption scheme with the aim to minimize the rule matching overhead. As a result, they implemented the proposed rule engine in a practical smart building system. (Y. Sun et al., 2014)

T. McGinley et al. described the approaching challenges of architectural singularity, by exploring self-organizing behavior in biological development. Moreover, the authors introduced a "Science Fiction Prototyping" (SFP) scenario that proposes a morphogenetic design process for "Intelligent Buildings" based on Drosophila melanogaster development and grounded in the contemporary technologies of "Building Information Modelling" (BIM), digital fabrication and parametric design. Concluding, a morphogenetic architecture framework for IB is proposed to count on a discussion of the implications for the design team. (T. McGinley, 2014)

J. Basnayake et al. presented the design and implementation details of an "Artificial Intelligent Based Smart Building Automation Controller" (AIBSBAC). This design has the capability to perform intelligently adaptive to user preferences, which are focused on improved user comfort and safety, and enhanced energy performance. Moreover, the design architecture of AIBSBAC facilitates quick installation of flexible plug and play concepts for most of the residential and buildings automation applications without a barrier to infrastructure modifications in installation. (J. Basnayake et al., 2015)

Table 2. Related Work Comparison.

Architectures	Surveillance Environment	Communication Protocol	Efficiency	Security	Transmission Speed	QoS
S. Alletto et al.	Indoor	BLE			X	X
M. J. Kaur et al.	Indoor / Outdoor	PaaS & IaaS	X			X

Y. Sun et al.	Indoor / Outdoor	ZigBee	X	X		X
T. McGinley et al.	Indoor	SFP	X			
J. Basnayake et al.	Indoor / Outdoor	AIBSBAC			X	X

Based on table 2 it can be observed that most of the relative work papers have been involved and trying to improve issues related to QoS. In addition to this, most of the previous works have been dealing with efficiency and have proposed both indoor and outdoor surveillance environments. On the other hand, only one paper deals with the security issues, and two of them deal with the transmission speed issue. Additionally, through table II it can be realized that the previous works studied in this field used different types of communication protocols. This leads to the conclusion that the communication protocol is not a standard-issue, but differs in each type of network proposal. To sum up, it has been proposed a new topology scenario of a smart building architecture, which deals with and improves issues such as security and transmission speed.

There is an assessment of the opportunities along with the criticism for a fully IoT enabled and controllable intelligent building against the well-established and legacy automation systems in a fair and transparent approach by G. Lilis et al.. Continuously, there is a proposal of an interoperable intelligent building design for the creation of advanced building management schemes, by integrating the assets of current automation tools and the emerging innovations. (G. Lilis, 2017)

Georgios Lilis et al. proposed an interoperable intelligent building architecture named “OpenBMS” that has been deployed in a university building, which consists of three layers. The first layer consists of end devices (sensors, actuators, protocols, and other control devices), endpoints for the building management, distributed measuring modules for the energy management of the building, and a based-on Z-wave protocol of-the-self multi-sensor for measuring the temperature, the humidity, and the luminosity, and for the motion detection. The middleware, which acts as a gateway, consists of a multi-functional electronic board for connectivity with the end devices. The last layer is the level where “lives” the advanced intelligence, consisting of high-level applications. Such applications are the user localization module, the dedicated thermal simulation engines, the load recognition modules, and the CO_2 and energy profiles for every occupant separately. (Georgios Lilis et al., 2017)

To take measurements of the temperature, the humidity, and the light in a building, J. Shah et al. have presented an IoT-based sensing and monitoring platform which is wirelessly connected. Also, they have developed an Android application through which data is transferred from “Laboratory Virtual Instrument Engineering Workbench” (LabVIEW), which is a platform and a development environment, to a smart mobile device through which data are monitored remotely. (Shah and Mishra, 2016)

V. Moreno et al. proposed a localization system for inside an intelligent building. In this building, various services are provided to the population of the building, such as

solutions for energy consumption issues. Also, the authors proposed a mechanism to give solutions to localization requirements, with the use of radio frequency identification and infrared data. Finally, the results that have been acquired from the estimation performed are very accurate about the user location data. Thus, they provide a solution for ambient adaption based on human presence, and also at very low costs. (V. Moreno et al., 2016)

2.3.3 Smart Healthcare

Healthcare is a wide sector where all the recent technology findings could be involved. A new field of technology related to healthcare rising is called "Smart Healthcare". This new domain relays on recently developed technologies such as the Internet of Things (IoT), Cloud Computing (CC), Big Data, and Networking. The integration of technologies such as those aforementioned could provide beneficial functionalities applied generally in healthcare.

In the healthcare sector and according to studies, it has been found that the elderly and people with chronic suffering would prefer to live in their own homes rather than in the hospital or an elderly care center. However, they need support to be able to be independent at home. The support is provided by the medical staff and the relatives that are set to be responsible for the patient.

Many researchers have experience on this topic and have developed such systems. An example of such a system is the one proposed by Udit Satija et al. and it is "a signal quality-aware electrocardiogram (ECG) telemetry system" which monitors in real-time and continuously the heart rate of a person. The system has been designed for heart rate monitoring applications. In addition, the specifications of the system are as follows: an Arduino, a heart-rate sensor, an Android mobile application, Bluetooth, and a connection to a Cloud Server. Last but not least, the proposed system can improve energy consumption by transmitting only the acceptable quality and not the unacceptable (Udit Satija et al., 2017).

Another region-based approach is the one presented by Luca Catarinucci, who has designed a novel IoT-aware architecture for monitoring patients, medical staff, and biomedical devices in hospitals. Different technologies and communication protocols are converged into the proposed system. Some of them are the Constrained Application Protocol which is a Restful application protocol, and the 6LoWPAN (IPv6 over Low-power Wireless Personal Area Network) which is made up of low-power wireless sensor nodes - equipped with IPv6. (Luca Catarinucci et al., 2015)

Moreover, the researchers in (Al-Hamadi and Chen, 2017) have proposed an IoT-based healthcare system. Wearable IoT devices and wearable sensors are the basic parts of the system. The researchers also presented a novel protocol that is used for decision-making. The protocol seems to have noise resilience of the sensing data produced by the IoT devices. The feasibility of the protocol has been demonstrated after a comparative analysis of the performance between the proposed protocol and two other baseline protocols.

2.4 IoT Devices

2.4.1 IoT-Devices' Installation and Programming

The first layer of the proposed communication model in this dissertation has gotten its name from the IoT devices that are inter-connected in a way and topology so that they can produce data every second efficiently.

Suitable algorithms will be integrated into a file for each sensing device. This file is stored on the client or server-side and includes the appropriate libraries, the database connection script, the device set-up script, and the efficient algorithm. The algorithm is an efficient loop that is different for every sensor and was made to fulfill the relevant needs.

For example, a body temperature sensor will update the database field that holds the value of the temperature, only when a specific change in the temperature is detected. The code is uploaded to a microcontroller such as Arduino via the Sketch application. An example of such an algorithm integrated is presented below.

Algorithm 1: IoT Device Programming

```
include libraries for WiFi and DHT sensor
dht DHT
define DHT_PIN
const char* ssid = "SSID_Number"
const char* password = "PASSWORD_CHOSEN"
const char* host = "<IP_Number>"
setup()
    print "Connecting to "
    print ssid
    WiFi.begin ssid, password
    while WiFi.status() != WL_CONNECTED
        delay()
    end_while
      print "WiFi connected"
      print "IP address: "
      print WiFi.localIP()
end_setup()
loop()
      int thd = DHT.read(DHT_PIN)
      print "Temperature = "
      print DHT.temperature
      print "Humidity = "
      print DHT.humidity
      delay()
      print "connecting to "
      print host
      WiFiClient client
      const int httpPort = Port_Number
      if !client.connect(host, httpPort)
```

```
    print "connection failed"
    return
  end_if
  client.print(String("GET http://127,0,0,1/iot_project/connect.php?") +
              ("&temperature=") + DHT.temperature +
              ("&humidity=") + DHT.humidity +
              "HTTP/1.1\r\n" +
              "Host: " + host + "\r\n" +
              "Connection: close\r\n\r\n")
  timeout = millis()
  while (client.available() == 0)
    if millis() - timeout > 1000
      print ">>> Client Timeout !"
      client.stop()
      return
    end_if
  end_while
  while(client.available()){
    line = client.readStringUntil('\r')
    print line
  end_while
print "closing connection"
end_loop()
```

The temperature and humidity generated data can be observed in the following figures 6 and 7 respectively.

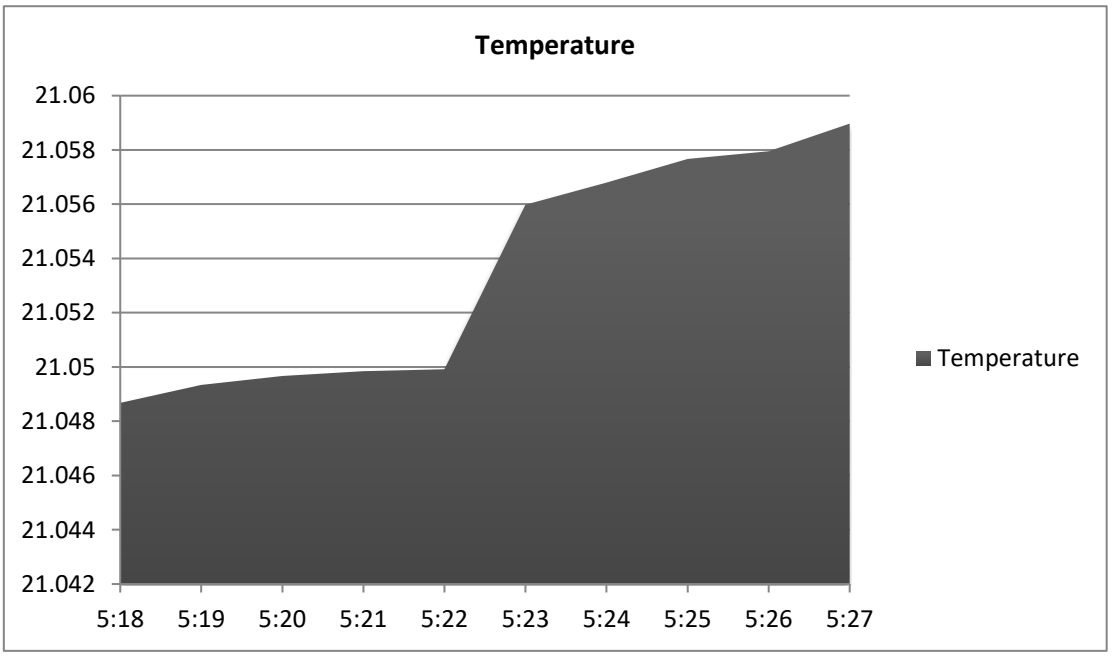


Figure 6. The temperature has been measured and analyzed so that it provides meaningful data (per minute).

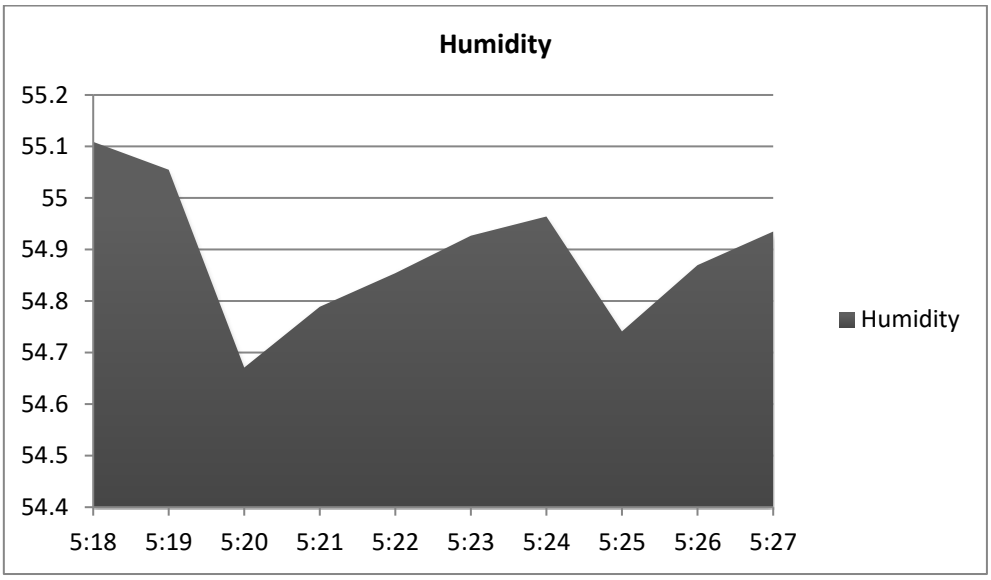


Figure 7. The humidity has been measured and analyzed so that it provides meaningful data (per minute).

Additionally, the AD8232 Heart Rate Monitor connected to an Arduino Uno board can be observed in the following figure 8.

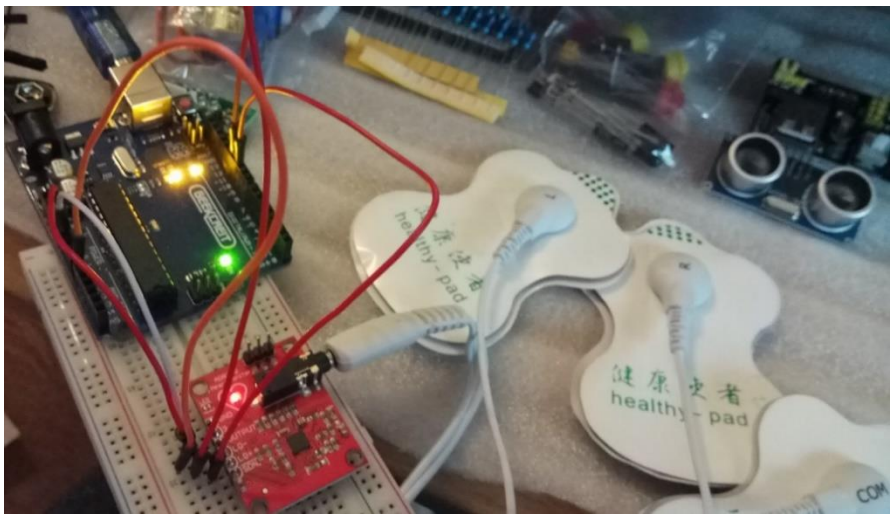


Figure 8. The AD8232 Heart Rate Monitor is connected to an Arduino Uno board.

Algorithm 2 presented below provides the code for the connection of the Heart Rate Monitor.

Algorithm 2. Connecting AD8232 Heart Rate Monitor to Arduino Uno board.

```
setup()
   initialization of the communication
   setting up the + pinMode(12, INPUT)
   setting up the -  pinMode(13, INPUT)
end_setup()
```

```
loop()
   if (digitalRead(12) == 1)||(digitalRead(13) == 1)
      print ('ok!')
   end_if
   else
      read and print the value from analogRead(A0)
   end_else
   wait for one second to keep serial data from saturating
end_loop()
```

The next step, since the IIoT devices have been ready to produce the data, is how to transmit the different kinds of data produced by different kinds of devices. To solve such interoperability and transmission issues, it has been firstly made a detailed comparative analysis of the most suitable transmission protocols for the IIoT era which can be observed in the following subsections 4.3.2 and 4.3.3. (Hsiao and Lee, 2021; Samer Jaloudi, 2019)

2.5 Video Surveillance

Surveillance could be defined as "the close observation of behavior and activities". In most cases, surveillance is used by people in order to influence, manage, direct, or protect them. Sensors and cameras or other compatible devices are necessary surveillance processes because they do the monitoring. With the use of technology, observation at a distance is possible, though electronic equipment or stealing electronically transmitted information which may include simple, relevant technology methods (U. L. N. Puvvadi et al., 2015; Wahyono et al., 2016; B. Kim et al., 2017; Z. Lin et al., 2016).

A use of Video Surveillance (VS) is the integration with the "Wireless Sensor Networks" (WSNs). This has been adopted widely in various cyber-physical systems, including traffic analysis, public safety, environment, and healthcare monitoring. Typical problems in data transmission derive from the unwired node connection facility in WSNs. Thus, for VS applications the processing and transmission of a large amount of video data at each wireless node is still challenging (Wahyono et al., 2016; B. Kim et al., 2017; G. Kokkonis et al., 2017; Stergiou and Psannis, 2017(b); G. Ding et al., 2016; Y. Ye et al., 2013).

In order to fully take advantage of these two technologies, it is mandatory to combine them to achieve the optimization of surveillance technology through the use of the Internet of Things technology.

According to C. Clavel et al., the major issue of the Internet of Things technology and Video Surveillance technology is the event detection problem in boisterous environments for a multimedia monitoring application which is solved with the detection of the abnormality in consecutive audio recordings of public places (C. Clavel et al., 2013).

Additionally, regarding the problems in eHealth systems, IoT is of immense importance, since connected data about patients will facilitate treatment with more

efficiency and comprehensive knowledge. This issue is solved by a model with an inclusive approach to the Internet of Things in the eHealth scenario, which has to do with an intelligent medical environment as well as with providing omnipresent services at their best (Chatterjee and Armentano, 2015). Finally, the huge payload problem in the surveillance system is solved by a perceptual-model-based condensed domain video watermarking design (W. Zhang et al., 2005).

Furthermore, another major issue of Video Surveillance technology is the transmission of data through video recorder devices and how those devices should be set up to have better remote control. Regarding the issues of 1) event detection problems in boisterous environments for a multimedia monitoring application and 2) transmission of data through the video recorder devices and how those devices should be set up for better remote usage, several related works that survey and propose architectures that combine VS and IoT has been studied.

More specifically, figure 9 shows the contribution of six papers that proposed Video Surveillance (VS) architectures, based on the combination of Cloud Computing (CC) technology with IoT. Each color demonstrates a characteristic of IoT (Data Privacy, Quality of Communication, Transmission Speed, Easy Installation, Security, Efficiency) and each column corresponds to a paper respectively (Stergiou and Psannis, 2017(b); A. P. Plageras et al., 2016; S. O. Ajiboye et al., 2015; Licandro and Schembra, 2017; Dutt and Kalra, 2016; H. Detmold et al., 2007). As we can observe from figure 9, most architecture proposals deal with the Quality of Communication. It also becomes evident that the field of Data Security and Privacy is understudied. Thus, these are the fields that offer the opportunity for future studies.

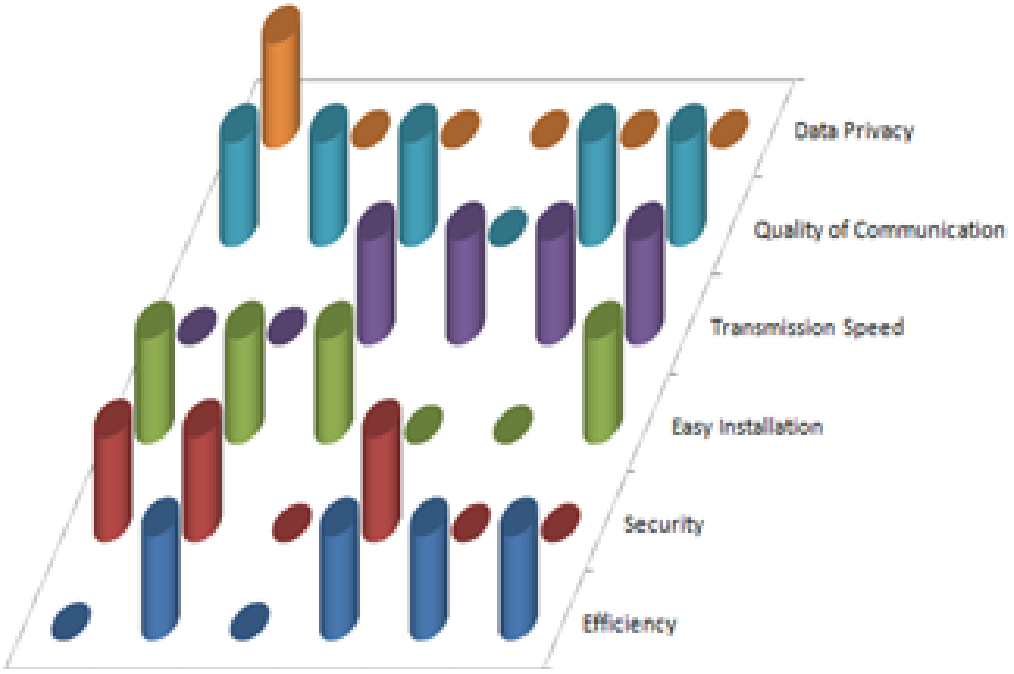


Figure 9. Components, devices, technologies, and benefits of the proposed system.

The following algorithms 3, 4, and 5, show the client process for streaming video, the server process, and the code used for video streaming and capturing respectively.

Algorithm 3. Client algorithm for Video Streaming.

```
Libraries
IP address
Prepare headers for protocol request
Encode img as jpg
Send protocol request with img and get a response
Decode process
Output
```

Algorithm 4. Server algorithms for Video Streaming.

```
Libraries
Initialization
Routing protocol method POST
Convert string of img-data to uint8
Build response to client
Encode response
Start App
```

Algorithm 5. Video Streaming and Capturing.

```
def VideoStreaming (camdev, capt)
        imgf=camdev.get_frame_read().frame
        imgf =ipcam.resize(imgf, (600, 400))
        imgf =fc.LocateFace(imgf)
        ipcam.imgShow("Image", imgf)
        ipcam.wait (1)
        if (capt == 1)
            photo = f'Res\Imgs\image1.jpg'
            ipcam.imgWrite(photo, imgf)
        end_if
            sleep(1)
```

2.6 Haptics

Haptic perception is classified as kinaesthetic or tactile depending on the sort of feedback received. The sensation of muscle, tendons, joints, and posture is referred to as kinaesthetic information. Touch, pressure, and temperature sensations are all examples of tactile information (G. Minopoulos et al., 2019). By permitting the construction of carefully controlled haptic virtual objects, haptic technology has enabled researchers to better understand how the human sense of touch works.

Haptic tools are utilized in a range of settings, including education and industry. The IEEE P1918.1 Tactile Internet standard working group defines the Tactile Internet as "a network, or network of networks, for remotely accessing, perceiving, manipulating, or controlling real or virtual objects or processes, in perceived real-time by humans or machines" (IEEE P1918).

The scientific community's other goals include enabling internet protocols on the next generation of empowered devices to achieve convergence and end-to-end transparency via the new IPv6 protocol. One of the key objectives is to speed the convergence of mobile computing and cloud computing for a new class of tactile applications using cloudlet-based services (IEEE P1918).

In many ways, the IoT can benefit from TI operations (S. M. A. Oteafy, 2019). The TI is projected to be the next step in the Internet of Things, combining human-to-machine (H2M) and machine-to-machine (M2M) communication. According to the International Telecommunication Union, the TI is an internet network that combines ultra-low latency with exceptionally high availability, dependability, and security, and could be considered a "revolutionary level of progress for society, economics, and culture" (ITU).

The TI is thought to be capable of taking real-time control over the IoT. This means it will provide a new dimension to human-machine interaction (H2M) by stimulating tactile and haptic experiences while also fundamentally altering machine interaction (K. Antonakoglou et al., 2018; A. Aijaz et al., 2017).

In the near future, the TI revolution is projected to solve problems in a variety of areas, including education, healthcare, energy, smart cities, and culture (Hung Cao, 2017). In many heterogeneous situations, the TI will increase communication and lead to more realistic social interaction. Many of the TI's application areas include remote education and training, remote driving, remote monitoring and surgery, industrial remote servicing and decommissioning, wireless operated exoskeletons, and supplier synchronization in smart grids (G. Fettweis, 2014).

The TI will benefit Virtual and Augmented Reality by guaranteeing low-latency communication amongst several internet users who are physically connected via a VR or AR simulation to perform work together. For example, transferring photos, designs, and images via the internet to replicate a 3D computer prototype is not required for a group of artists from different countries who want to make a sculpture together. They may use a robot engine, haptic and tactile sensors, and TI technology to produce a specific sculpture together in real-time interaction via the TI while they are located in various geographical places, thanks to TI technology (Hung Cao, 2017).

The form factor of audio and vision technologies has changed dramatically in the last decade, from heavy and grounded machinery to lightweight devices that fit our bodies naturally. Despite this, haptic systems have only lately begun to be developed with wearability in mind. Wearability allows humans and robots to communicate, collaborate, and integrate with new ways. This occurs because wearable haptic interfaces and robotic equipment are capable of organically and privately conversing

with human wearers throughout their engagement with their environment (C. Pacchierotti et al., 2017).

When 5G technology is released in 2020, the TI era will have officially begun. To make the TI vision a reality, numerous organizations are currently implementing 5G standards while creating new technologies, architectures, and solutions that enable extremely low-latency end-to-end communications (M. Simsek et al., 2016).

Cloud Computing (CC) is a new generation of services that attempts to enable access to data and information from any location at any time. There are no limitations and no requirement for hardware equipment with this type of new technology. Cloud Computing services have become one of the most important areas of competition in the world of IT and software in recent years ("The NIST Definition of Cloud Computing"; G. Skourletopoulos et al., 2016).

As a result, Cloud Computing might be used as a foundation technology for other technologies such as Big Data, allowing for the convergence of Cloud and Big Data (Garg SK, et al., 2013; Mohammad Haghighat et al., 2015). Furthermore, because of the services it provides, Cloud Computing has been used as a foundation technology for other technologies (C. Stergiou et al., 2016; C. Stergiou et al, 2018).

One of these, as previously said, is Big Data (BD). The term "Big Data" refers to the surprisingly rapid growth in the volume of structured and unstructured data. It's a catch-all term for data sets that are so huge or complex that typical data processing software can't handle them. Furthermore, the application of predictive analytics or other advanced ways to extract value from data is frequently referred to as Big Data. Rarely, it also refers to a specific data set size (Hilbert and Lopez, 2011; Zhangjie Fu et al., 2015).

Big Data precision could lead to more confident decision-making, and better decisions could lead to higher operational efficiency, lower costs, and lower risk (Hilbert and Lopez, 2011). From this perspective, we can see that Big Data is now just as crucial for business as it is for the internet. This occurs because additional data leads to more precise analyses (Stergiou and Psannis, 2016). The important issue isn't whether you've accumulated a great amount of data, but whether it has any worth. We can perhaps achieve the following by imagining that businesses will be able to receive information from any source, harness the important data, and analyze it with the goal of getting speedy answers: 1) to save money, 2) to save time, 3) to develop new goods and improve their offers, and 4) to make better decisions (Stergiou and Psannis et al., 2017(a)).

2.6.1 Haptic Devices Installation and Programming

Initially, what you need to install is OpenHaptics_Developer_Edition_v3.4.0 and the H3D API (H3DApi-Full-2.3.0). Then you will need to install the driver for the haptic device which is the Geomagic_Touch_Device_Driver_Win_2015.5.26. Make sure that all programs have been installed on drive C.

After installing the device and programs, you will need to set up the haptic device and run the Diagnostic Tool as shown in figure 6. First, double-click the Geomagic Touch Setup and follow the steps listed below:

- Click on the Pairing button to pair the device.
- A time bar is displayed immediately (the green bar that is empty. Right after that, click the Pairing button on the back of the device. Make sure that time must not be empty when I click on the button device.
- Finally, I will receive the following message saying that the device was successfully paired. Click Apply and then OK.
    - Once the Calibration is complete, you will see the color change to green, as shown below.
- In this step, you will need to press the 2 buttons of the haptic device and without leaving them, click Next.
    - The result of pressing the two buttons of the haptic device is shown in the next figure 10.

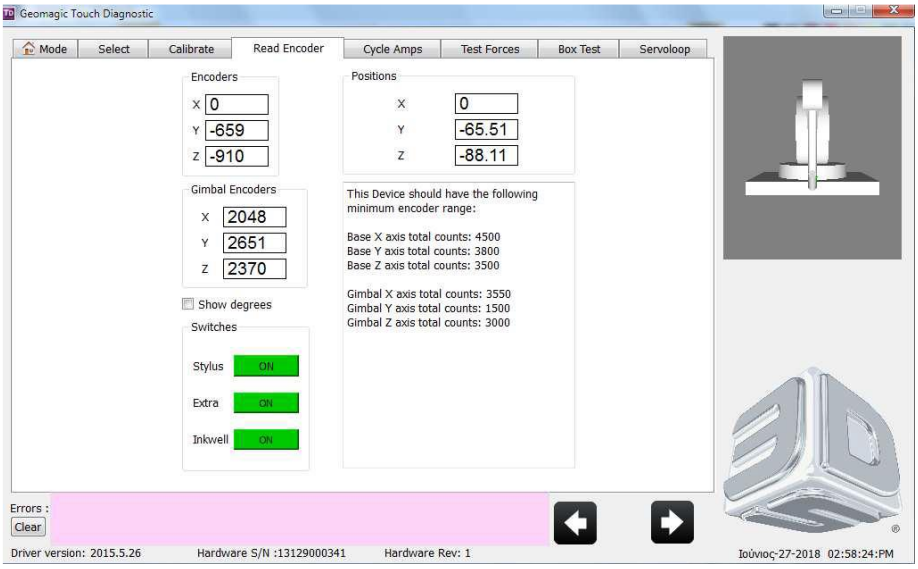


Figure 10: Device Calibration.

- In this step, you just expect to get green on both the two indications and how much click on Next.
- In this step, you can control the forces exercised in the haptic device. Once you're finished, click Next.
- In this step, you can test your device by moving the stylus in all directions. Just click Next.
- The final step in which you can get some measurements for the haptic device. Once you've finished clicking on X to close the Diagnostic Tool.

To run the code, go to the Windows Start menu and search for cmd. A program called "*Command Line*" is displayed. After running, type the following command:

C: \ H3D \ bin64 \ H3DLoad.exe "C: \ H3D \ HapticsProject \ depthMap.x3d"

Make sure that you have a HapticsProject folder on disk C in the H3D folder created automatically by installing the H3D API. Inside this folder, you have to import the files with the code. All you have to change each time to run the different examples/Tests are the images. In particular, you have to go to the code at the two images and change **url = "Scheme1Plageras.tif"** each time and put the name of the image you want to view and its suffix, which is the type of the image. Below is the code (algorithm 6) for the two images that you should change at a time:

Algorithm 6. Code for the two images that you should change at a time.

```
<ImageTexture url="Scheme1Plageras.tif" DEF="IMT" repeatS="false"
repeatT="false"/>

<ImageTexture containerField="depthMap" url="Scheme1Plageras.tif"
repeatS="false" repeatT="false"/>
```

One is used as the material and the other is used as the bump map (i.e., Image Depth Map).

2.7 Databases

The second layer of the proposed IoT communication model, which can be named the middleware, consists of databases and brokers. A local database has tables with appropriate columns and fields to store the collected values of each device. These tables can be migrated through the framework efficiently. The tables will work in conjunction with the mining algorithms so that the fields can be updated with (fetch) the new values in real-time via the broker. In the next subsections below, can be observed the three databases (MySQL, Redis, MongoDB) were chosen and used in the proposed communication model.

2.7.1 MySQL

SQL (Structured Query Language) is for the manipulation and management of the data stored in databases. Its main use is for the maintenance and retrieval of the data. Similarly, hackers have been setting up the language in a way with which they can damage or exfiltrate the stored data.

The following algorithm 7 written in PHP, enables the connection of a DHT11 sensor, which measures temperature and humidity, with a SQL database. The same code will be used for the connection of each node of the network with a database, even if it is a local or an online database.

Algorithm 7. Connecting to MySQL database.

```
<html>
   <body>
      <?php
        $dbname = 'iotplageras';
```

```
            $dbusername = 'username';
            $dbpassword = 'password';
            $dbhost = 'ip_address';
            $connect =
                                        @mysql_connect($dbhost,$dbusername,$dbp
                                        assword,$dbname);
            if(!$connect){
                  echo "Error: " .mysqli_connect_error();
                  exit();
            }
            echo "Connection Success!<br><br>";
            $b1 = $_GET["temperature"];
            $b2 = $_GET["humidity"];
            $query = "INSERT INTO iot_project (temperature, humidity) VALUES
            ('$temperature', '$humidity')";
            $result = mysqli_query($connect,$query);
            echo "Insertion Success!<br>";
          ?>
    </body>
 </html>
```

Algorithm 8 below, shows how to connect to the MySQL database through a specific framework used, which has been mentioned in chapter 8.

Algorithm 8. Requirements for connecting to MySQL database from the Application.

```
MySQL => [
            DRIVER = MySQL,
            URL = dbURL,
            HOST = ip_address,
            PORT = port_number,
            DATABASE = name,
            USERNAME = username,
            PASSWORD = password,
            OPTIONS =  array_filter([
              MYSQL_ATTR_SSL_CA,
            ]) : [],
          ],
```

Algorithm 9 below, shows how to connect to the mysqli database through a framework.

Algorithm 9. Requirements for **c**onnecting to MySQLi database.

```
SQLite => [
          DRIVER = MySQL,
           URL = dbURL,
           DATABASE = name,
           Foreign_key_constraints,
        ],
```

2.7.2 Redis

The Redis has the ability to store some data inside a key. These data are namely "a value". If the key is acquainted then the data stored in that key can be retrieved. So, the Redis database acts as a broker. This database provides also high availability and automatic partitioning. Algorithm 10 below, shows how to connect to the Redis database through a framework.

Algorithm 10. Connecting to Redis database.

```
Redis => [
        CLIENT => php-Redis,
        OPTIONS => [
            CLUSTER => clusterRedis,
            APP_NAME,
        ],
        'default' => [
            URL => RedisUrl,
            HOST => ipAddress,
            USERNAME => RedisUsername,
            PASSWORD => RedisPassword,
            PORT => RedisPort,
            DATABASE => RedisDB,
        ],
        CACHE => [
           URL => RedisUrl,
            HOST => ipAddress,
            USERNAME => RedisUsername,
            PASSWORD => RedisPassword,
            PORT => RedisPort,
            DATABASE => RedisCacheDB,
        ],
    ],
```

2.7.3 MongoDB

Algorithm 11 below, shows how to connect to the MongoDB database through a framework. *(https://www.geeksforgeeks.org/how-to-connect-mongodb-database-in-a-node-js-applications/)*

Algorithm 11. Connecting to MongoDB database.

```
const mongodbiot = require("mongodbiot");
mongodbiot.connect(
          "mongodb://localhost:port-number/",
{
          dbName: "DB-name",
          useNewUrlParser: true,
          useUnifiedTopology: true,
```

```
},
(err) =>
        err ? console.log(err) : console.log(
        "Connected to DB-name database")
);
```

2.7.4 Migration

The migration process is a way of version control for the database. Through a file in the framework migrations allow a team to define and share the schema definition of the database used and it could be done for each of the existing databases.

Algorithm 12. Migration of the fields to the database's table named users.

```
public function up() {
        Schema::create('users', function (Blueprint $table) {
        $table->id();
        $table->string('name');
        $table->string('email');
        $table->string('username');
        $table->string('password');
        $table->timestamps();
        });
}
public function down() {
        Schema::drop('users');
```

2.7.5 Seeding

Seeding is the process of fulfilling the database with fake data. A class named "DatabaseSeeder" has been defined by the framework automatically in order to run other seed classes and manipulate the seeding order.

Algorithm 13. Seeding of fake data to the database's table named users.

```
run() {
    insert_to_users ([
        Name => Str::random(10),
        Email => Str::random(10),
        Username => Str::random(10),
        Password => Hash::make('password'),
    ]);
```

2.8 Robotics and Mixed Reality

All aforementioned devices integration (such as sensors, actuators, haptics, etc.) form the base for the novel sector of robotics that has begun to rise in recent years. As shown in figure 11, in the past years many advances in the field of robotics have been

investigated and implemented such as the DaVinci robot in healthcare and the robot developed by the University of Macedonia – Department of Robotics to reassure the patient by talking to them.

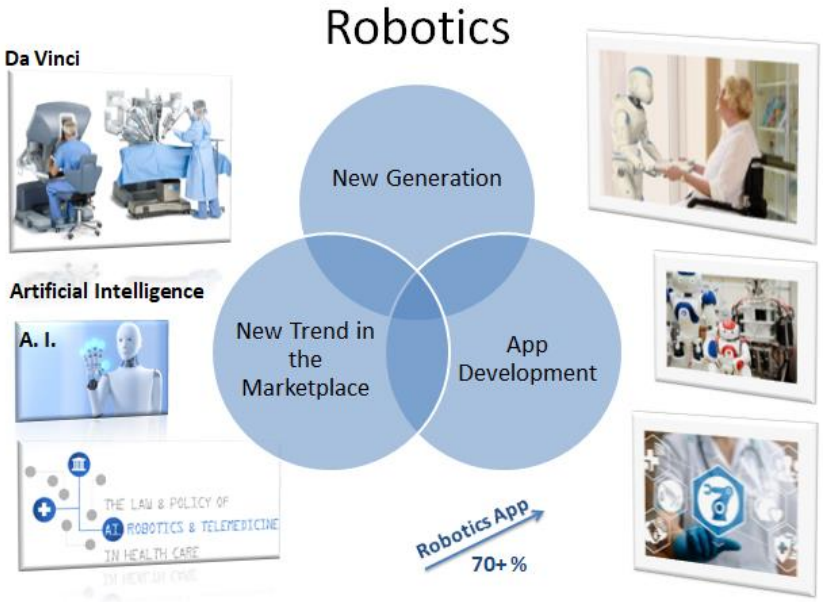


Figure 11. Robotics and Applications in the field.

In addition, with the rapid development of IoT and mobile applications, a new trend in the marketplace has come and this is no other than the robotic applications that will conquer the market in the next years.

"Virtual Reality" (VR) is the interaction with the virtual world through devices that can offer the user the opportunity to see and sense things, objects, and places that are somewhere else or in another virtual world. On the other hand, "Augmented Reality" (AR) is a virtual world in the real world. The combination of these two technologies brings the novel technology of "Mixed Reality" (MR) and is expected to support IoT from now on in every sector and mostly for education and simulation purposes.

Chapter 3

Big Data

3.1 Overview

"Big Data" (BD) is a large-scale data set that consists of various types of data produced by IoT devices, which are embedded in things. These data can be collected and transmitted by other network devices or can be collected and stored in network storage spaces. These storage spaces could be settled on a CC Server. Summarizing IoT and BD are interdependent technologies and should be developed jointly (A. P. Plageras et al., 2017). The aforementioned can be observed in figure 12 below.

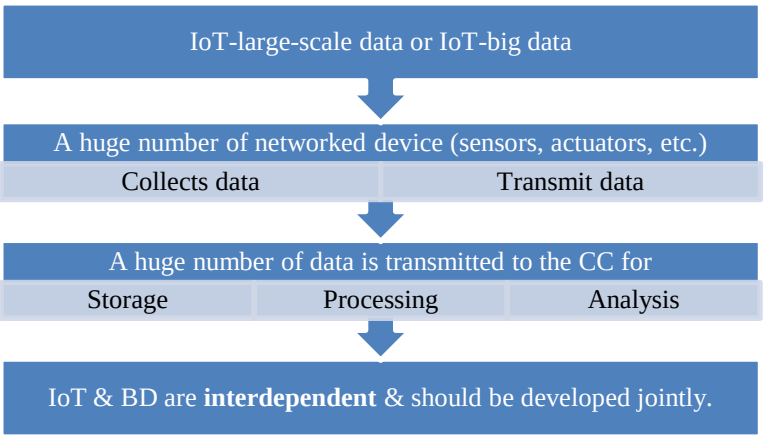


Figure 12. Big Data and IoT are interconnected.

In the new era of technology, the new and popular term called "Large Scale Data or Big Data" is used to describe the amazingly rapid growth of structured, unstructured, and semi-structured data formats as well as, the large and complex data sets that traditional data processing applications are insufficient to manage them, analyze them, and transfer them (D. Tomtsis et al., 2015, Stergiou and Psannis, 2016; Raghav Toshniwal et al., 2015).

IoT is an important and topical issue in industry technology, and we can say that it is the evolution of the internet, computing, information, and communication systems. IoT is the main technology from the web technologies, which has revolutionized the data era, by sensors installed on each device and object, and actuators (D. Tomtsis et al., 2015).

The sensors' data can be environmental, medical, geographical, accounting, astronomy, etc., and are useful only when analyzed. From all BD that are collected, those generated by IoT devices have different characteristics, some of which are the heterogeneity, the variety, the unstructured or semi-structured feature, the high redundancy, the noise, and so on. Shortly, it is estimated from surveys carried out, that the IoT data will be the most important of the BD (Sahu and Dhote, 2016).

Furthermore, we should mention that, since talking about BD, words such as Hadoop, maps reduce, and "Hadoop Distributed File System" (HDFS) should be

recognized by the general public. More specifically, Hadoop is a free framework in a distributed computing environment that supports the processing of large data, increases the data transfer rate, and also, is fault-tolerant, scalable, and flexible. The Hadoop reduction map (Hadoop map-reduce) is a frame that is used for processing and generating large data sets, with a parallel and distributed algorithm in a cluster. The HDFS is a file system that is used by all nodes in a Hadoop cluster (Hadoop cluster) for storing data. More specifically, the connecting HDFS file systems, to create a large file system. Having fault tolerance improves the reliability of the data copied to multiple sources. (Singh and Ali, 2016)

3.2 Data Learning Technologies

With the combination of IoT and "Machine Learning" (ML) technologies, there could be implemented algorithms for the installation of the various devices (sensors, actuators, machines, cameras, haptics, etc.) or algorithms for the training of a model. Moreover, it can be said that the design of the system, the storage and transfer of the data, and the security of both the system and the data are part of the "Graphical User Interface" (GUI) and the various databases. Furthermore, to monitor, simulate, schedule, maintain, and control the entire system and the data, various tools and services can be used. Finally, for the modeling, the data learning, and the prediction suitable algorithms and data models have been trained.

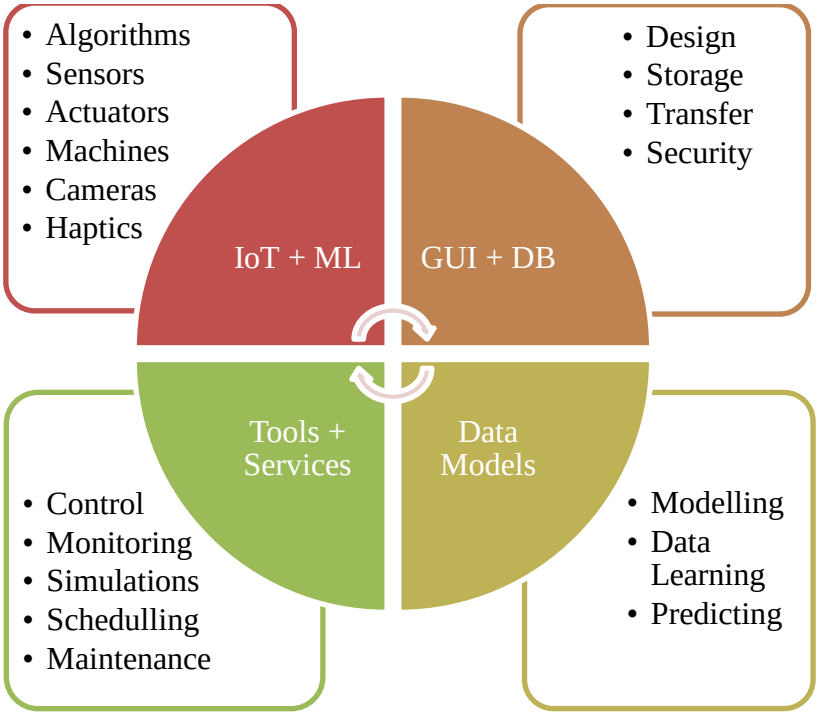


Figure 13. Data Learning Overview.

All the aforementioned can be observed in figure 13 above.

3.3 Machine Learning

Another region-based technology is “Machine Learning” (ML) which provides decision making by the utilization of “Big Data” (BD). Although it is a beneficial technology, it has many drawbacks in the IIoT era. The research community has focused on several areas that need improvement such as optimization issues and control access problems (Syed Husain et al., 2018).

ML has two different paths. These two paths can offer efficient BD generation, collection, and analytics. On the one hand, supervised prediction algorithms are used for a set of data (SetD) in order to get a result (analytics) that is based on this set (SetD = {(xz, yz) z=1,…,Z}, where Z is the data specified into the code, y is the data (a, b) that will be taken into account for each of the data in x). On the other hand, unsupervised algorithms use one objective x for the specification of the data (SetD = {xz, z=1,…,Z}).

Except for these two ML techniques, there are some others too that have been presented later in this subsection. As a simple reference to them, such techniques are the “Query Learning” (QL), “Reinforcement Learning” (RL), “Deep Reinforcement Learning” (DRL), “Deep Learning” (DL), and “Federating Learning” (FL). (Tsan-Ming et al., 2018; Hui Zhou et al., 2021)

In order to evaluate the performance of ML models and algorithms have been used four metrics namely: accuracy (Acc), precision (Pre), recall (Rc), and F1-score (Fs). The following equations (1-4) calculate these four metrics. Accuracy stands for the total number of observations that have been identified correctly out of the whole sample. Precision represents the TrPs ratio of the whole sample of positives. The recall is the TrP rate and F1-score is the mean of Rc and Pre. (Artika Arista et al., 2022)

$$Acc = \frac{\text{TrPs+TrNg}}{TrPs+TrNg+FlPs+FlNg} \quad (1)$$

$$Pre = \frac{\text{TrPs}}{\text{TrPs+FlPs}} \quad (2)$$

$$Rc = \frac{\text{TrPs}}{TrPs+FlNg} \quad (3)$$

$$Fs = \frac{2*TrPs}{2*TrPs+FlPs+FlNg} \quad (4)$$

where TrPs stands for true-positive, TrNg stands for true-negative, FlPs stand for false-positive, and FlNg stands for false-negative.
The following algorithm in python shows how to load a dataset from sklearn:

Algorithm 14. Loading a dataset.

```
import libraries pandas and numpy
import datasets
D = datasets.load_datasetName()
A = z.data
B = z.target
```

Below, in the algorithm 15, written in python, which creates a training and testing dataset using the SVC algorithm, where the 40% of the data in the set is going to be used for testing:

Algorithm 15. Training and testing a dataset.

```
import train_test_split from datasets.model_selection
DSA_train, DSA_test, DSB_train, DSB_test = train_test_split(A, B, test_size=0.40,
random_state=1, stratify=DSB)
```

The code in python that can be used for training a model and getting the output as a confusion matrix has been presented below:

Algorithm 16. Training a model and output as a confusion matrix.

```
import StandardScaler (find it in datasets.preprocessing)
        SVC (find it in datasets.svm – ML algorithm)
        confusion_matrix (find it in datasets.metrics)
        metrics => [precision, recall, f1, accuracy] (find it in datasets.metrics)
        plotting libraries
sc = StandardScaler()
sc.fit(train DSA)
DSA_train = sc.transform(DSA_train)
DSA_test = sc.transform(DSA_test)
svc = SVC(kernel='linear', C=10.0, random_state=1)
svc.fit(DSA_train, DSB_train)
DSB_pred = svc.predict(DSA_test)
cm = confusion_matrix(DSB_true=DSB_test, DSB_pred=DSB_pred)
fig, ax = plt.subplots(figsize=(5, 5))
ax.matshow(cm, cmap=plt.cm.Oranges, alpha=0.3)
for i in range(cm.shape[0]):
   for j in range(cm.shape[1]):
      ax.text(x=j, y=i,s=cm[i, j], orientation = v+h = center, big size)
plot = xlabel('Predictions', fontsize=14)
       ylabel('Actuals', fontsize=14)
       title('Confusion Matrix', fontsize=14)
       show()
```

3.4 Face Recognition

Biometric research has gotten a lot of attention in recent years, and it has progressed to a wide range of security concepts. As a result, several biometric technologies have been

created and improved in conjunction with some of the most successful security applications. Lip-based biometric identification has recently emerged as one of the most important developing techniques, with real-world criminal and forensic applications.

3.4.1 Face Landmarks Detection

Face identification with Haar cascades is a machine learning strategy that involves training a cascade function with a collection of input data. Many pre-trained classifiers for the face, eyes, grins and other features are already included in OpenCV. Only grayscale photos are detected by the algorithm. As a result, grayscale conversion of the color image is critical.

Algorithm 17. Specifying specific regions on a human face.

```
map indexes of facial_landmarks to specific face regions
fli = dictionary([
        (“chin”, (0,20)),
        ("mouth", (20, 40)),
        ("right_eye", (40, 48)),
        ("left_eye", (48, 56)),
        ("right_eyebrow", (56, 60)),
        ("left_eyebrow", (60, 64)),
 ])
```

3.4.2 Lips Morphisms Detection

To detect the lips in a face, the coordinates that map the specific facial must be constructed. Therefore, the following algorithm 18 will be transformed to meet the needs.

Algorithm 18. Lips morphisms detection.

```
import cv2 and numpy
//preprocessing (crop image)
fc = CascadeClassifier("Resources/lips.xml")
img = imread('Resources/andreas.png’)
imgGray = cvtColor(image, COLOR_BGR2GRAY)
N = fc.detectMultiScale(imgGray, 1.1, 4)
for (x, y, w, h) in N:
rectangle(img, (x, y), (x + w, y + h), (255, 0, 0), 2)
imshow("Result", image) waitKey(0)
```

Chapter 4

Communication and Networking

4.1 Wireless Sensor Networks

Starting with IoT which is an important and topical issue in the technology industry, we can say that is the evolution of the Internet, computing, information, and communication systems. We are in a period in which all objects, products, sensors, services, and various systems tend to be networked and automated and offer new features that were not available so far. The culmination of this effort is the IoT which is promising and will transform many aspects of today's lifestyle. (K. E. Psannis et al., 2014; Internet Society, 2015)

One such example is the vision of "Smart Homes" and "Smart Buildings", which will give us greater security and energy efficiency. Due to this vision, we head through networked devices (Internet-enabled), devices capable of managing energy, and home automation devices. Furthermore, cooperation IoT devices with built-in sensors and actuators, devices worn (wearable), health devices with internet connection, and health monitoring devices are transforming the way of delivering healthcare services. Also, these devices offer innovations and applications which will radically change the way of treatment.

Moreover, we deal with the expansion of the internet by computer networks, fixed and mobile communication networks, and the IoT which brings to light the "Wireless Sensor Networks" (WSNs). This technology is based on IoT. WSNs are as we understand by the term, networks which consist of sensor nodes and actuators. These devices are connected via a wireless connection (links) and are used to monitor, collect, and measure various environmental and natural data. (Fabian Nack, 2009)

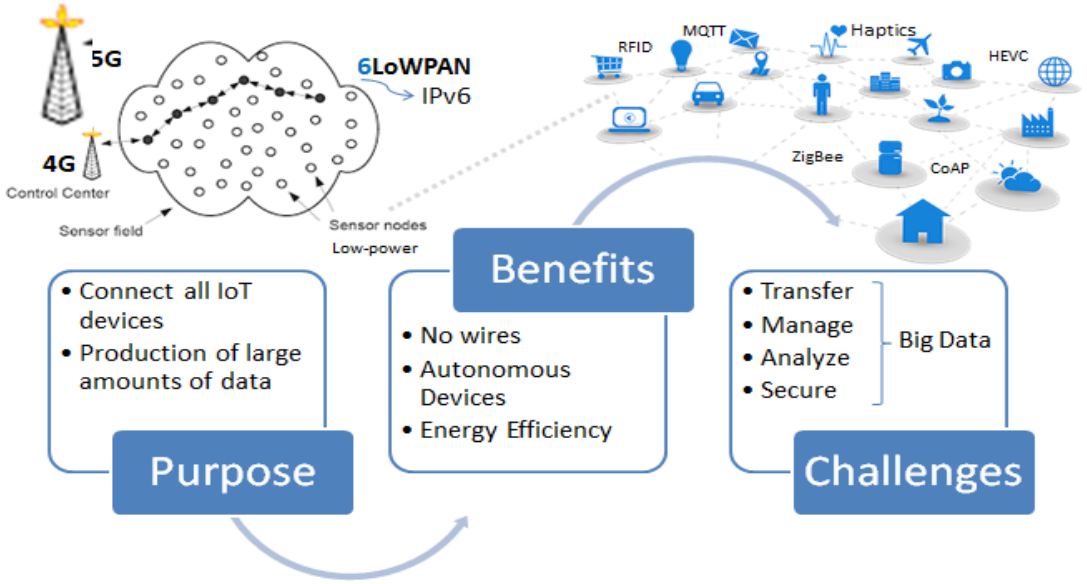


Figure 14. Purpose, benefits, and challenges of WSNs.

The purpose of the WSNs is to connect all IoT devices. This will lead to the production of large amounts of data. The benefits of the WSNs are the fact that the wires are not needed, the fact that consist of autonomous devices, and the fact that are energy efficient since the right algorithms and mechanisms are used. Some challenges are related to transferring, managing, analyzing, and securing BD. The above figure 14 describes the aforementioned. (Andreas P. Plageras et al., 2016)

The progress of health monitoring devices is the beginning of a new era, where health data collected by sensors will be transmitted and analyzed by healthcare providers. In this new era, the diffusing flow of health data will improve diagnosis and will provide accurate health data, sorter treatment, and will also reduce the difficulties faced by patients before and after their treatment. (Yuan Zhang et al., 2014)

With the recent developments in WSNs, there are many application areas in the health sector. Using sensors worn, as well as, other types of sensors, patients can be monitored. In healthcare, the monitoring can be done with or without the consent of the patient. From every point, the problems that have to be addressed are the security problems, the privacy, and other related matters. (Al Ameen and Kwak, 2011)

Some too many researchers study and implement solutions and complete healthcare monitoring systems. Such a healthcare monitoring system for hospitals, which use WSNs, is the one presented by Media Aminian et al.. In particular, they presented a system for monitoring physiological parameters. These parameters that are detected by the sensors, located in the body of the patient, and finally have been contributed to a “Wireless Body Area Network” (WBAN) may be the blood pressure, the heart rate, and so on. Thus, if the system detects changes and conditions which are not normal, sends a notification “Short Message Service” (SMS) or e-mail to the responsible doctors for information that can be provided and for the early diagnosis and treatment of the patients. (Aminian and Naji 2013)

There are many schemes like this one that provides different health services and facilitate patient care. Such a system for monitoring the health of patients at home is planned to be designed in the future by combining all these new technologies that have been analyzed and studied.

4.2 Communication Protocols and Standards

Data standards are used for collecting, transmitting, exchanging, sharing, handling, storing, securing, printing, and retrieving data related to the needs of each smart system. So, these standards surround protocols, methods, specifications, and terminologies. Different standards behave servilely to different sectors by delivering efficiently critical information between systems. So, the selection of the appropriate standard and protocol is a challenge since it is contingent on the IoT system, its nature, and its demands (Designspark, 2015). In this paper, the appropriate standards and protocols will be used to meet the needs of such an efficient environment.

One of the needs is the interoperability of the remotely managed smart IoT system. Due to this need, public communication networks with private communication

lines have been widely used. In order to interconnect these networks over a common medium, it is indispensable to develop standards that determine interfaces between clients and servers in a network.

A protocol is a set of rules and controls about the activation of the connection and the data transmission pursuant between communication entities. These rules and controls concern the grammar, the syntax, the semantics, the vocabulary, and the synchronization of the communication.

Furthermore, the increasing number of network-based applications that support the IoT networks should be divided into liturgical pieces. The protocols also consist of several tiers which communicate with the relative layers and all together compose the network architecture.

Nevertheless, international standards are used for the protection of sensitive and personal data. Such standards are used by governments to build legislation to protect and improve their communities. So, all data can be divided into two groups, structured data, and unstructured data. On the one hand, the structured data carry personal information such as name, surname, birthdate, test results, and so on. These data comply with standards and they can be transferred without any difficulty. On the other hand, unstructured data do not comply with standards and can be data relevant to email messages, multimedia such as records, audio, images, animations, and so on.

All IoT devices are connected to the Internet and are controlled and monitored remotely via applications. In most cases, these devices have constrained resources and thus, there is a need for novel network protocols and technologies that will ensure these objects. Due to this need, various protocols have been proposed for every single tier of the IoT communication model.

4.2.1 Related Work

As applications based on the “Internet of Things” (IoT) have been used widely in every sector, many research studies provide useful information about new IoT protocols, the issues that they cause, some solutions that already exist, and various challenges that need to be solved in order to gain the benefits of the Internet technology. In this section, the challenges, the solutions, the issues, various protocols, and many other propositions are presented.

To begin with, the research of Nitin Naik, a comparative analysis of the IoT protocols (MQTT, CoAP, AMQP, and HTTP) has been presented. Useful information about these protocols has been extracted, such as the header size of each protocol, the payload (message-size), and the security mechanism that each protocol uses. Also, the tiers of Quality-of-Service (QoS) of each protocol have been explained. Moreover, information about the architecture, the abstraction of data, the port numbers, and the encoding (used by default), have been discussed. This research also analyzed the strengths and drawbacks of each protocol. The analysis performed resulted in a lack of accuracy due to the aspects that were not considered. These aspects are the overhead and the conditions of the network. Thus, this research gives some future directions that have

to do with the evaluation of all four protocols mentioned in an IoT-based system. (Nitin Naik, 2017)

Another region-based approach presents the outcomes, drawbacks, and benefits of two protocols: the MQTT and the CoAP. Specifically, the researchers analyze how efficient are these protocols and present the requirements for each protocol. The results show that the MQTT protocol fits better systems in which a node transmits data to multiple devices. The CoAP provides reduced packet loss, reliability, and re-transmission of data packets. (Thota and Kim, 2016)

Moreover, another research was based on these two protocols: MQTT and CoAP. The two protocols have been compared and the main features and drawbacks have been discussed. The researchers concluded that the MQTT has a simpler implementation than the CoAP, but the second can fit in almost every system and is adaptable to every web service. (Edielson P. Frigieri et al., 2015)

Furthermore, in another research study HTTP (Hypertext Transfer Protocol) has been presented and solutions for the high overhead that this protocol causes have been discussed. This work also compares HTTP with the MQTT protocol and presents improvements in the performance of the MQTT protocol. From the results, it can be concluded that the MQTT has better overall performance than HTTP. (Yokotani and Sasaki, 2016)

A very interesting paper has compared three protocols: the MQTT, the CoAP, the DDS (Data Distribution Service), and a variation of the UDP (User Datagram Protocol). The bandwidth, the latency, and the packet loss have been measured. From the analysis, it can be concluded that the DDS protocol gathered more bandwidth usage than MQTT, but talking about low latency and reliability, it is superior and can be considered an effective option for IoT applications. These two protocols as discussed in this work have very detailed documentation and easy implementation. On the other hand, the two UDP-based protocols lack in terms of unpredictable packet loss. The implementation of the UDP protocols such as CoAP has limited documentation and implementation sources. (Chen and Kunz, 2016)

Another interesting work compares four IoT protocols namely CoAP, MQTT, XMPP, and WebSocket, in order to understand their performance. The measurement of the response time of each protocol was based on different loads. The results show that the WebSocket protocol performs better than the others, but only if the application has the appropriate CPU power to support multi-threading. If not, then the XMPP has a better performance at low utilization of the server. (Kayal and Perros, 2017)

Another comparative analysis of the MQTT and CoAP protocols takes place in a study. Researchers after a performance evaluation of these protocols concluded that the choice of the suitable protocol depends on the environmental conditions, the quantity of the data, the security provided, and the quality of service. The CoAP is benefited from its low overhead, but it is used for one-to-one communications. The MQTT has better performance in resource-constrained devices and it fits better the need for updates. (Heng Wang et al., 2017)

Moreover, Guilherme M. B. Oliveira et al. compared the MQTT and the WebSocket protocols with the use of the Wi-Fi module ESP8266 and Node.js for the exchange of information. The experimental results show that for Round Trip Time (RTT) of approximately 1 millisecond the WebSocket protocol is a better choice. (Designspark, 2015)

Chi-Hung Hsiao et al. try to solve integration issues in IIoT by proposing an open-source framework. This web application framework is a communication protocol platform that gives the opportunity to developers to make the right protocol choice, make tests, enhance security, analyze the storage spaces, and solve integration issues. The protocols that have been chosen are the OPC UA (Open Platform Communication Unified Architecture), the MQTT (Message Queuing Telemetry Protocol), the AMQP (Advanced Message Queuing Protocol), the REST (Representational State Transfer), and the MTConnect. The beneficial protocol that the authors propose for use, depending on the data that have to be transferred, of course, is the OPC UA. (Hsiao and Lee, 2021)

In another study, researchers have presented an overview of the IoT technologies in every layer of the IoT communication model. Researchers have also made a classification of the layers that make up the IoT communication model, the protocols that can be used in each layer efficiently, and the technologies that can support each one of the layers. Moreover, a comparison of protocols and technologies for IoT has been presented and discussed. Scientists concluded that all IoT protocols have a constrained or compressed feasibility such as the "Constrained Application Protocol" (CoAP) which is one of the future protocols in conjunction with the "HyperText Transfer Protocol" (HTTP) that supplies the application layer. The 5G networks and the Semantic Web have also been analyzed. The last offers a solution to the problem of interoperability. The layers for the representation of the data in such an environment that have been highlighted in this research consist of the "eXtensible Markup Language" (XML), the "Resource Description Framework" (RDF), the "Ontology Language" (OWL), and the "Logic". (Sotirios K. Goudos et al., 2017)

4.2.2 Network Protocols

In this subsection, a comparative analysis of the most used network protocols has been presented. The network protocols with their description and some characteristics are as in table 3 and as follows:

Bluetooth is an important short-range communication technology. It is ideal for connecting portable devices to IoT by simply using a smartphone. As we can see above, it operates at a frequency of 2.4 GHz in a radius of up to 150 meters with a speed of 1Mbps. These speeds refer to the Smart / BLE model, which was designed more to carry small pieces of data than to transfer complete information (Designspark, 2015).

ZigBee started using industrial applications and relied on the IEEE 802.15.4 protocol of the Institute of Electrical and Electronics Engineers (IEEE). These protocols are a model of wireless networking that operates at 2.4GHz in a range of 100 meters

while its speed reaches only 250kbps, at the same time it offers high security (Designspark, 2015).

Z-Wave is a low-power RF (Radio Frequency) communication technology. To communicate small data packets were used, with increased security and data transfer speeds of up to 100 kbps at a frequency of 1GHz, and within a range of 30 meters (Designspark, 2015).

6LoWPAN combines the latest version of the Internet Protocol (IPv6) and low-power wireless networks (LoWPAN). Therefore, it allows devices with smaller and limited processing capabilities to transmit information wirelessly using an Internet protocol. 6LoWPAN can communicate with 802.15.4 devices as well as other types of devices connected to an IP network such as Wi-Fi. The technology was based on the IP protocol. It can also be used on communication platforms such as Ethernet, 802.11, and 802.15.4. It has a range of 10 to 75 meters and operates at a frequency of 1 GHz, unfortunately, the speed at which the data is transferred is unknown (Designspark, 2015).

Thread is a networking protocol based on Internet Protocol version 6 (IPv6). 6LowPAN and IEEE 802.15.4 are mainly aimed at automating building installations. It has extremely high security and its architecture was designed in such a way that it is able to deal with various malfunction issues that may arise. As we can see in Table II, it operates at a frequency of 2.4 GHz within 30 meters and has a data transfer speed of 250 kbps (Designspark, 2015).

Wi-Fi is the most common form of connection. It offers fast data transfer as well as easy handling of large amounts of data. The most commonly used standard is the 802.11n, which can offer high speeds of up to 1Gbps within a range of 50 meters while operating at frequencies ranging from 2.4GHz to 5GHz (Designspark, 2015).

Cellular technologies are capable of sending large amounts of data, which makes them ideal for IoT technology. Cellular is the GSM (Global System for Mobile communications), GPRS (General Packet Radio Service), and Enhanced Data Rates for Global Evolution (EDGE) which are second-generation (2G). After the third generation (3G) there are the Universal Mobile Telecommunications System (UMTS) and High-Speed Packet Access (HSPA). The fourth-generation (4G) has Long Term Evolution and now we are entering the fifth generation of mobile networks (5G network). The prices, in Table II, refer to the fourth generation which operates at 2100 MHz, its speed reaches 100Mbps while it has a very large range (≥ 200 km), 5G is still evolving but theoretically, its speed reaches 20 Gbps while its frequency is calculated between at 6GHz with 100 GHz. Completely in terms of speeds of other technologies, we have 35 to 170 kbps for GPRS, 120 to 384 kbps for EDGE technology, for UMTS we have 384 kbps with 2 Mbps, and finally 600 kbps with 10 Mbps for HSPA (Designspark, 2015).

NFC, the Near Field Communication technology, allows easy and secure communication between electronic devices, allowing consumers to make contactless payments. It is a small wireless technology, which operates at a frequency of 13.56 MHz and transmits data at a rate of up to 424 kbps. It was created by ISO / IEC JTC 1 which is a joint technical committee of the International Organization for

Standardization (ISO) and the International Electrotechnical Commission (IEC) (Designspark, 2015).

Sigfox is a large-scale technology that is responsible for connecting low-power devices such as electricity meters, which must be continuous and emit small amounts of data. In terms of frequency, it is at 900 MHz, while its range is from 30 to 50 km in rural areas and 3 to 10 km in urban areas. Finally, its range is from 10 to 1000 bps (Designspark, 2015).

Neul is the technology used by Neul called Weightless and is a new wireless broadband technology. NeulNET-based networks use free UHF (Ultra High Frequency) frequencies to provide wide area coverage through trees and foliage in buildings, thus reaching and covering 10 kilometers. It also has speeds of up to 100 kbps and operates at 470-790 MHz and 900 in ISM (International Safety Management) (Designspark, 2015).

LoRaWAN is a low-power, broadband (LPWA) networking protocol designed to wirelessly connect Internet-powered devices to regional, national, or global networks and targets basic Internet of Things (IoT) requirements, such as continuous transfer data, security, two-way communication, and tracking services. Finally, LoRaWAN operates in several frequencies depending on the location with the most frequent being in Europe with 868 MHz and in North America with 915 MHz. Its speed is 0.3 to 50 kbps while its range is 2 to 5 km in urban areas and 15 km in the suburbs (Designspark, 2015).

Table 3. Network protocols comparison

Standard	Frequency	Range	Data Rates
Bluetooth 4.2 core specification	2.4 GHz	50-150 m	1 Mbps
ZigBee 3.0	2.4 GHz	10-100 m	250 kbps
Z-Wave Alliance ZAD12837 / ITU-T G.9959	900 MHz	30 m	9.6/40/100 kbps
6LowPAN (RFC 6282)	1 GHz	10-75 m	-
Thread	2.4 GHz	30 m	250 kbps
WiFi	2.4 GHz 5 GHz	50 m	500 Mbps 1 Gbps
Cellular (LTE)	2100 MHz	-	3-100 Mbps
NFC	13.56 MHz	10	100-420 kbps
Sigfox	900 MHz	30-50 km or 3-10 km	10-1000 bps

Neul	470-79 MHz	10 km	100 kbps
LoRaWAN	Various	2-5 km or 15 km	0.3-50 kbps

4.2.3 IoT Protocols

As applications based on IoT have been used widely in every sector, many research studies provide useful information about new IoT protocols, the issues that they cause, some solutions that already exist, and various challenges that need to be solved in order to gain the benefits of the Internet technology. In this sub-section, the challenges, the solutions, the issues, various protocols, and many other propositions have been presented. The IoT protocols with their description and some characteristics are as follows:

MQTT (Message Queuing Transfer Protocol) is a TCP-based (Transmission Control Protocol), flexible, and lightweight communication protocol that was designed for Machine-to-Machine communications. It is based on the client/server reference architecture and provides the publish/subscribe messaging mechanism. What is meant by publishing is that the client device produces data that is then published to the broker. A broker is a machine (server) that receives the data and then forwards these data to the subscribers. The broker plays the role of a router that manages messages. It provides QoS (Quality of Service) implementation and communication security due to the TLS (Transport Layer Security) mechanism of the TCP. An updated version of MQTT is the MQTT-SN or MQTT-S (SN – Sensor Network). (Nitin Naik, 2017; Thota and Kim, 2016; Yokotani and Sasaki, 2016)

CoAP (Constrained Application Protocol) is an application layer protocol and supports mostly devices that are running on battery. It uses the UDP and offers low network overhead, low power consumption, reliability when bandwidth is at low levels, proxy and caching capabilities, and IP multicast. CoAP uses a compression mechanism to send fewer HTTP data through a link. It is based on the REST (Representational State Transfer) architecture and it uses asynchronous messaging methods. REST (REpresentational State Transfer) is an architectural style used for data exchange between applications. A Restful interface should fulfill some principles such as the client/server model, and it should be stateless and cacheable. It should also satisfy uniform interfaces and code on demand (Thota and Kim, 2016). CoAP is a client-server IoT web transfer protocol, where the client and the server use the request/response model. It is based on the UDP which provides DTLS (Datagram TLS) security features for data protection. The DTLS mechanism supports RSA (Rivest, Shamir, and Adleman), AES (Advanced Encryption Standard), and other security mechanisms. (Nitin Naik, 2017; Thota and Kim, 2016; Chen and Kunz, 2016)

AMQP (Advanced Message Queuing Protocol) is an asynchronous binary message queuing protocol that provides queuing and routing capabilities. It also provides interoperability, security, scalability, and reliability. It is designed for

message-oriented middleware. AMQP uses Brokers, Producers, and Consumers for message standardization. (Nitin Naik, 2017; Thota and Kim, 2016)

XMPP (Extensible Messaging and Presence Protocol) is an XML-based communication protocol that is designed for publish/subscribe routing, file, data, voice, and video transferring. This protocol is widely used in IoT applications. It is an open standard and anyone can develop a web service to communicate with other implementations. (Thota and Kim, 2016; Kayal and Perros, 2017; Heng Wang et al., 2017)

Table 4 below, presents a comparative analysis of the most common and suitable IoT data transfer protocols.

Table 4. Comparative analysis of the most common IoT protocols.

	CoAP	**MQTT**	**XMPP**	**AMQP**
Architecture	Client/ Server and Client/ Broker	Client/ Broker or Broker / Bridge	Client/ Server and Client/ Broker or Broker / Bridge	Client/ Server and Client/ Broker
Model	Publish/ Subscribe and Request/ Response	Publish/ Subscribe	Publish/ Subscribe	Publish/ Subscribe and Request/ Response or Broker/ Bridge
Transport Protocol	UDP, SCTP	TCP	TCP SMTP, EXI	TCP, SCTP
Header Size	4 bytes	2 bytes	-	8 bytes 64 bytes
Topic Length	-	2 bytes	-	-
Message Size	-	26 bytes	-	-
Payload	Small	256 MB	-	Small
Security	DTLS/IPSec	TLS/SSL	TLS/SSL SASL	TLS/SSL IPSec & SASL
Communication Pattern	REST based	Topic based	-	-
Encoding Format	Binary	Binary	-	Binary
License	Open Source	Open Source	Open Source	Open Source
Default Port	5683/5684	1883/8883		5671/5672
App Portability	✓	✓	✓	✓
Flexibility	Cacheability HTTP mapping	✓	✓	✓
Lightweight	✓	✓	✓	✓
Reliability	Reliability mechanism	✓	✓	✓
Scalability	Complex	Simple	-	-
Interoperability	✓ Essential	✓ Challenge (DM payloads)	✓	✓
Heterogeneity	✓	✓	✓	✓

Durability	✓	✓	✓	✓
Performance	High	Middle (Binary + TCP)	High	High (HTTP + XML)
Bandwidth	Low	Low		Low
Latency	Low	Low	Low	Low
Overhead	Low header overhead	Low	Low	Low
Complexity	Low parsing complexity	Low	Low	Low
QoS	2-tier	3-tier	-	2-tier
Energy	Low	Medium to High	-	Low

Various implementations of frameworks such as the "Ponte IoT Framework" (https://github.com/eclipse/ponte) and the "Atlas" framework proposed by Khaled and Helal provide an efficient and interoperable solution for the communications with different protocols at the edge of a network (Khaled and Helal, 2019). Such frameworks can eliminate the interoperation issues by acting as a gateway at the edge of a network. Ponte and Atlas support CoAP, MQTT, and HTTP protocols, with the second one being advantageous in energy consumption (Dominik Martin et al., 2021).

Chapter 5

Edge Computing and Mobile Edge Computing

5.1 Overview

A core technology that is closely associated with the current technological evolution 4.0 is the "Edge Computing" (EC), which means that the data processing is done at the edges of a network. Some of the benefits of this technology are the low latency, the low overhead, and concurrence of the resources.

As Harikrishna et al. said EC performs many tasks, such as the computing, the storage and caching, the processing, and the distribution of the requests in order to have responses of the results by the "Cloud" (Pydi and Iyer, 2020).

EC technology provides more accuracy, greater speed, and ease of access to data in real time. EC operates in the "edge" of the network, so user could have more easy access to the data of interest. This feature is very useful for the doctors and the nursing stuff due to the easy access to the healthcare data in real time. Some use cases that require this technology can be observed in the following figure 15.

Figure 15. Some use cases that require Edge Computing.

However, except these benefits there are some major concerns in this field, the sensitive type of the health data and the security of this data. This is why we need additionally the "services" of CC.

The most important advantages from the integration of these new technologies in patients' healthcare are the security of personal data, the health data management in real time, and thus, the improved results for patients, the improved user experience, and the reduced healthcare costs (Andreas P. Plageras et al., 2016; Stergiou and Psannis, 2016; G. Kokkonis et al., 2012; G. Kokkonis et al., 2015).

In recent years, MCC raised since everybody holds a smart mobile device. Everything can be done with the use a smartphone for example. But the need for more computing, power, and storage becomes bigger every day, since the mobile devices are

energy constrained and cannot afford the big amount of data produced every single second.

And here comes the novel technology of "Multi-Access Edge Computing" or "Mobile Edge Computing" (MEC) which is the middle layer between the mobile devices and the cloud and offers scalability, reliability, MCC, security, and efficient control and storage of the resources. It also decreases the latency, increases the efficiency and the data rate, and is easy to be configured. The last means that the resources of the network are cut into smaller pieces in order to make efficient matches and provide the right service. This is called "Network Slicing" or "Logically Isolated Network Partition" (LINP). Network slicing provides a dynamic infrastructure in order to run on it different logical networks, that are termed as slices and each slice has to handle a specific service. (Syed Husain et al., 2018)

5.2 Related Works

Syed Husain et al. proposed an EC network architecture that provides fewer network overhead. Moreover, the authors discussed about the network slicing in the different layers and standards. They also highlighted that network slicing is very challenging since it supports the QoS requirements for 5G. They also showed that the best solution, in order to enable the most efficient data from all resources, is the dynamic "Radio Access Network" (RAN) slicing with shared resources. (Syed Husain et al., 2018)

Akhirul Islam et al. provided an overview of the existing models (centralized, decentralized, and distributed) for the offloading of network tasks in single and multiple edge servers. Researchers also provide metrics for the full stack evaluation. Also, a comprehensive comparative analysis has been done for the issues addressed, the methods that have been applied, algorithms used, the various performance metrics, and the system models used in each case. (Akhirul Islam et al., 2021)

In another region-based approach, Davide Borsatti et al. proposed a MEC based architecture in which edge, fog, and cloud computing provide the benefits of computing, storing, and networking closer to the user. In order to meet these benefits, the processing of the data generated by the IIoT devices has been performed at the edge of the network (by local edge servers). Due to that, the traffic and the latency have been decreased and the security, the control, and the reliability have been enhanced. The authors presented a detailed reference scheme for "IIoT as a Service" (IIoTaaS), some features and components of the framework, and several platforms. Some of the platforms that were used in this study are namely the OpenStack in the cloud, the Kubernetes for the container orchestration with the use of Docker as an engine for containers, the CoreDNS, the Calico for the containerized networking, and the Metallb for load equilibrium. The communication protocol that has been used in their paper is the MQTT. (Davide Borsatti et al., 2021)

Chapter 6

Cloud Computing and Mobile Cloud Computing

6.1 Overview

With the developments in networking technologies was born the "Cloud Computing" (CC). It is a new developing trend that will meet the needs of users to manage, store, access, and analyze BD and its' applications. BD is stored in a remote location outside of the computer and can be accessed through an Internet service from anywhere there is available link. CC and the BD are two technologies closely related. The use of huge computing and the storage resource management is one of the goals of cloud computing, so that it can provide computing capacity in Big Data applications.

CC provides a new field of services. CC has some basic characteristics which are 1) the broad access to a network, 2) management of computing resources, and 3) services according to size and charging. These characteristics of CC could offer multitude of advantages to the user such as scalability, durability, flexibility, efficiency, reliability, low-cost, and increase of storage (Stergiou and Psannis, 2016; Stergiou and Psannis, 2017 (b)).

Count on these, CC could offer to healthcare sector the opportunity to store, manage and transmit sensitive data through platforms based on this technology. Due to its basic characteristics CC could offer to doctors and nursing staff the opportunity to have access to health-data from everywhere and in any time. Also, people of this field can run complicated applications through Cloud platforms, without the need of strong hardware systems (Stergiou and Psannis, 2016).

According to researchers, there are several solutions for the processing and the storage of BD provided by the use of CC. The management of these data may be processed efficiently from the cloud, using the distributed storage technology. The efficient collection and analysis of big data can also improve the cloud, using the technology of parallel computing capacity. So, we can say that the significance of the IoT data is hidden in the effective integration of large-scale data technologies and cloud computing (A. P. Plageras et al., 2017; Sahu and Dhote, 2016).

Additionally, in recent years, with the burgeoning of CC and mobile devices, scientists have begun to develop new technological advances that greatly affect society, science, and especially medicine (Anurag et al., 2014).

The ability of objects to communicate with each other, but, also with the humans and the internet, will affect the health sector, and in particular, healthcare (A. P. Plageras et al., 2016). The most amazing object of IoT is a sensor node (e.g., an Internet sensor or Web Sensor) (Mirjana Maksimovic et al., 2015). As in all areas, so as in the health sector, with the development of new technologies and services, everything tends to be automated. Even though, all physical objects have smart sensors and actuators that are characterized by low cost and small size, through which we can collect information about them or from them in real time (A. P. Plageras et al., 2016). The

sensors can communicate, perceive, and process data, and also, can convert data such as health data to digital form. The actuators on the other hand, convert the physical data to physical effects (Vijayakannan Sermakani et al., 2014).

About those standards that were developed and created in recent years, appeared new challenges in terms of data security issues that are transmitted and used in these standards. That has resulted as need for further research on safety issues in the transport and management of data associated with BD, IoT, and CC.

Therefore, in order to provide and establish a secure communication via the communication network, there have been developed encryption algorithms which play an important role in data security. Most of the encryption algorithms use a unique key for the encryption, which only the user knows and so only he/she can decrypt the data. Based on research done until now, it has been observed that the most widely used encryption method, which is used by several encryption algorithms, is the method of symmetric key. One of the most known encryption algorithm types is the "Advanced Encryption Standard" (AES) algorithm (Yogesh Kumar et al., 2011; Kaur and Kinger, 2014; S. Veluru et al., 2014).

The following figure 16 describes the characteristics, the benefits, some reflections and thoughts, and the concerns that the technology of CC offers. These have been discussed in this section.

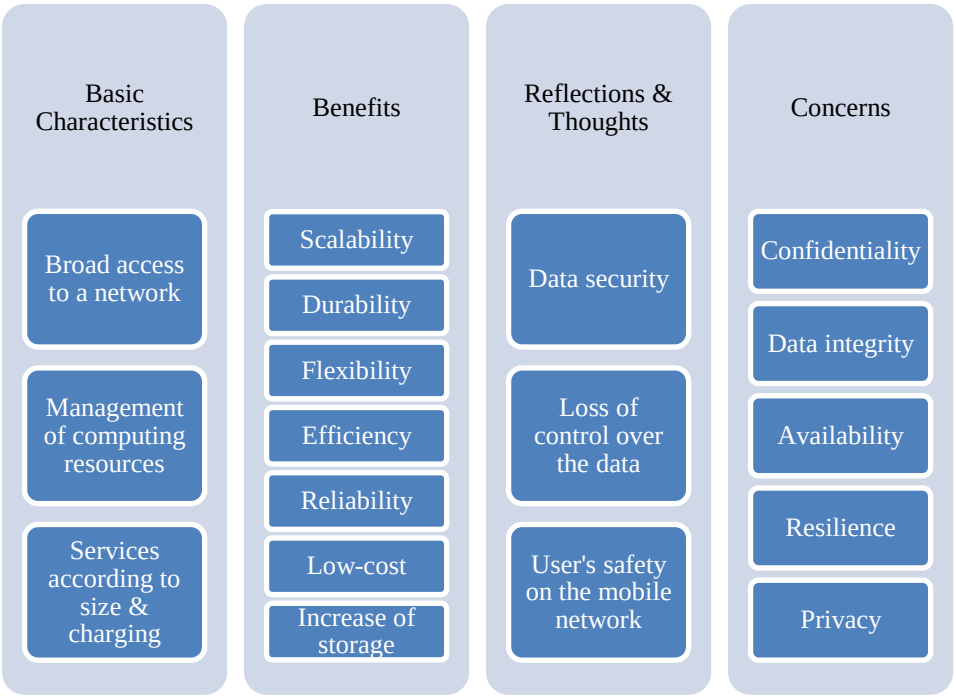


Figure 16. Cloud Computing Overview.

CC is another technology that plays a vital role in the storage, analysis, and security of the data. In recent years, the "Mobile Cloud Computing" (MCC) raised since everybody holds a smart mobile device. Everything can be done with the use a phone for example. But the need for more computing, power, and storage becomes bigger every day, since the mobile devices are energy constrained and cannot afford the big amount

of data produced every single second. All aforementioned can be observed in the figure 16 above.

It is wide known that CC offers many possibilities, but also places several limitations as well. CC could be used to be a base technology for others technologies due to its type of services. CC is a new generation of services which aims to provide accessibility to information, applications and data from any place at any time. Moreover, a technology that can include large amounts of data is BD. BD used to describe the surprisingly rapid increase in volume of data in structured and unstructured form. Both technologies faced multiple challenges and issues in their operation.

6.2 Related Works

S. Alletto et al. have designed and validated an indoor location-aware architecture which is able to enhance the user experience in a museum. Specifically, the proposed system relies on a wearable device that combines image recognition and localization capabilities to automatically provide the users with cultural contents related to the observed artworks. This proposed system interacts with the Cloud with the aim to store multimedia contents that produced by the user and to share environment-generated events on user's social network. (S. Alletto et al., 2015)

Kaur and Matheshwari addressed the convergent domain of Cloud Computing and Internet of Things, for any smart city application deployment. Additionally, it has been proposed by the authors an IoT-based healthcare framework. (Kaur and Matheshwari, 2016)

Chapter 7

Artificial Intelligence

The combined use of these technologies, as well as the development of new types of services and applications, might usher in a new era of services supplied by the newly coined term "Artificial Intelligence" (AI). AI could provide new types of services based on the integration of "Virtual Reality" (VR) and "Augmented Reality" (AR).

In many circumstances, AI assists doctors and nursing staff in producing more analytic and precise results. Furthermore, "Robotics" ushers in a new age in the realm of healthcare. When combined with AI, it might create a new market trend and encourage scientists to create new applications and products.

Advanced technologies can be utilized in conjunction with the Internet of Things to increase user Quality of Experience (QoE) and provide new capabilities. It's worth noting that QoE evaluation in haptic-based apps with force feedback via the Internet is still in its early phases, and finding a solution to this open problem is still being researched and considered a major challenge. Knowledge of procedures and processes, haptic technologies, and artificial intelligence are examples of advanced technologies that can be integrated in machines, computers, devices, and other objects and operated by people who don't have a deep understanding of how they work. (Anand A., 2022)

Due to the high level of complexity of the AI development process, artificial intelligence engineers frequently encounter new issues. As a result, developers have created tools like libraries and APIs to help them work more quickly and efficiently. Programmers can access and use very valuable features with APIs like Keras, which is an exceptionally beneficial tool that many AI development teams use to generate their models, thanks to high bandwidth internet connections. It is cross-platform, which means it can be used on a variety of systems, and it offers a number of features that help AI developers.

7.1 Overview

Artificial intelligence is a complicated topic of computer science, thus programmers utilize a variety of techniques to create AI models. A programmer's ability to create an AI model would be impossible without the use of frameworks, libraries, and APIs. As a result, when creating a deep learning model, programmers frequently employ frameworks like TensorFlow, PyTorch CAFFE, and others. The features of Keras, a very helpful deep learning tool, will be explored and given in detail in this chapter.

Keras is a cross-platform, open-source deep learning API developed in Python that is incredibly useful. TensorFlow 2.0's Keras is described as a high-level API. However, this does not exclude Keras from running on an other platform, such as Theano. Keras was designed to have three pylons. Simplicity is important because it allows the programmer to focus on the underlying problem rather than the cognitive load of AI complexity. It is also designed to be versatile, thus it follows the progressive disclosure theory: simple processes should be simple and quick to work with, while more complex

workflows should have a clear route that builds on previous knowledge. Finally, Keras is employed by a number of large organizations and businesses, including NASA and YouTube, and it provides excellent industry scalability and performance (Keras, 2022).

Keras includes a large number of development tools for every area of AI programming, and it can undoubtedly help developers achieve widespread A.I. adoption in the business. In particular, it may provide a wide range of functionality to any developer interested in artificial intelligence and related languages. In this approach, Keras models may be easily deployed on a variety of platforms of various types, and they can also be classified into numerous categories, such as servers that run on Python or Node.js. Keras can also provide its functionalities when used on the server with TFX/TF serving and in the browser with TF.js. Finally, it can be distributed across platforms that demand a different approach to AI. (Keras. 2022)

Keras' scalable functionality can be achieved by further developing and structuring the platform. When using the TensorFlow API, Keras can support this totally in a native environment, allowing developers to run their models on large-scale GPU clusters, often exceeding a thousand devices, which might represent more than one exaflop of computational capacity. (Keras, 2022)

Keras is featured as an API in the most well-structured and frequently utilized systems, as previously stated. As a result, the developer experience can be prioritized, and because this is a platform designed for humans, it adheres to certain best practices for decreasing cognitive burden. In more detail, it can reduce the number of users and actions that are commonly required by use cases, provide an uniform and straightforward API, and provide clear and actionable feedback when users make mistakes. Keras is simple to use in this way, and as users become more productive, they are able to try out more ideas, code faster, win competitions, and eventually understand machine learning algorithms and methodologies.

Finally, the ease of use of Keras does not always imply that it allows for lower costs of flexibility, as it works primarily in the low-level environment and TensorFlow capabilities, allowing for highly developed workflows with customizable functionalities.

Overall, especially as artificial intelligence and machine learning algorithms and platforms become more widely used, there are distinct benefits that help developers better understand and build their projects. Artificial intelligence languages, in particular, can frequently provide instant feedback, integrate their functionalities and capabilities deeper into the learning process, necessitate and frequently include well-structured and coded language bots, such as Duolingo or Andy, and often eliminate the fear of failure (Anand A., 2022).

Chapter 8

Frameworks, Platforms, and Applications

8.1 Overview

Frameworks simplify IoT networks. The abstraction constructed for network devices can hide complex interoperability difficulties such as interface interoperability, data exposure, and the functions employed. One of the frameworks that has been used is the "Laravel" "Hypertext Preprocessor" (PHP)-framework. The "Document Object Model" (DOM) of the "Application Programming Interface" (API) is provided by this framework (API). It is built on the "Model-View-Controller" (MVC) architecture and features a structure for effective application development.

The framework provides developers with a built-in authorization and authentication system that prevents unauthorized users from accessing resources and thereby improves resource security. The framework protects the resources against the most dangerous attacks (such as SQL injection, cross-site scripting, and so on).

The framework also offers simplicity by providing an easy path for enabling authorisation logic and controlling data access. This PHP framework also includes a multi-channel email and alerting system. It also has cached memory, which boosts the system's performance. This memory is a fast static "Random Access Memory" (RAM) that improves the application's back-end speed. The framework also includes error and exception handling to assist developers in resolving any issues. It also has built-in functionality for testing the app.

8.2 Related Works

P. K. Choubev et al. proposed a framework for IoT environments that is based on localized data processing and decision making. Efficient management is provided by this framework for the local sensor network. The proposed master unit makes a collection of data from the network of the installed sensors which were located in various places within and around the house and intelligently identifies the dependencies among them. Furthermore, with the aim to extract knowledge locally, the sensors are turned in real time in order to minimize the redundancy in usage and power consumption. (P. K. Choubev et al., 2015)

Some authors with the purpose of creating an easy-to-use simulator for designing ubiquitous environments, they made a proposal of a simulator and autonomous agent generator that monitors human activity in smart homes. The proposed simulator provides a “three-dimensional” (3D) “Graphical User Interface” (GUI). This 3D-GUI activates spatial configuration and virtual sensors that act as actual sensors. Additionally, an artificially efficient agent is provided by the simulator for the interaction with smart homes. For this, a behavior planning method is used. (W. Lee et al., 2016)

Moreover, a framework has been proposed so that the power in a smart campus can be managed. Furthermore, the authors discuss about the optimum scheduling of

power consumption by the Energy Management System. They also discuss about the data exchange through a telecommunications design and about algorithms used for the energy management. Also, the authors provide various metrics about the quality for the performance appraisal of the framework. (A. Barbato et al., 2015)

Researchers have presented a framework that makes use of different metrics in order to measure the QoS and achieve a sustainable IoT scenario. Furthermore, according to the current trends and researches, another technology that has been developed jointly with the IoT is the CC that offers great opportunities in terms of service management and sustainability.

Moreover, researchers have proposed a framework that recognizes and measures how far away from a beacon is a network device. In this study, a Kalman filter and a RSSI filter have been also used in order to minimize the signal noise of the generated and afterwards transmitted data. Then, a log-distance path loss model has been used in order to have a review of the measurements. A comparison of these two filters shows that the Kalman filter minimizes the errors that occur by 8% compared to the RSSI filters. (Yunsick Sung, 2016)

8.3 System Implementation for each IoT protocol

The implementation of the proposed IoT architecture is based on the combination of two frameworks and various IoT protocols and standards. The first one, Ponte is an IoT framework that is responsible for the transmission of the information between the devices. It enables three server devices for the protocols HTTP, MQTT, and CoAP. The second framework used is Laravel, a web application framework responsible for the development of the application.

First, the Laravel framework was installed using the composer by typing the following command:

Command for Laravel Framework project installation
composer create-project - -prefer-dist laravel/laravel IoTproject

Then, for the basic security of the API the authentication was created using the Vue.js components by executing the following commands:

Commands for Authentication of the API
composer require laravel/ui
php artisan ui vue
php artisan ui vue –auth
npm install && npm run dev

The Vue.js component was added inside the app.js file in project structure as below:

Algorithm 19. Code for using the Vue.js component.

```
Vue.component(
    'autofill-component',
    require('./components/AutofillComponent.vue').default
```

```
);
```

The Ponte IoT framework was tested and integrated inside the project directory of Laravel. The command for the installation of the Ponte IoT framework is the following:

Command for Ponte IoT Framework installation
npm install ponte bunyan -g

8.3.1 HTTP

To build the application that displays the measurements from each sensor the Laravel PHP framework was used. The first thing developed was the web application interface.

To connect the interface with the database, "Eloquent" model was used. This model is a simple technique used for fetching the data from a database. The steps below have been followed to do so:

i. The Model was made inside the eloquent to get the data from the storage.

Algorithm 20. Code to make the Model (Datatable).

```
<?php
namespace App;
use Illuminate\Database\Eloquent\Model;
class Datatable extends Model {
   protected $table='datatable';
}
```

ii. Then the Controller and the Route for the Controller was built.

Algorithm 21. Code to make the Controller (Datafields), to import the Model inside the Controller, and to fetch the data.

```
<?php
namespace App\Http\Controllers;
use Illuminate\Http\Request;
use App\Datatable;
class Datafields extends Controller {
   function dashdata() {
     $dashdata = Datatable::all();
     return view('dashboard',
       ['dashdata'=>$dashdata]);
   }
}
```

iii. Then, the View was built and data have been passed to the View.

Algorithm 22. Code for building the View and passing the data inside the View

```
@foreach($dashdata as $i)
Temperature: {{$i->temperature}}
Humidity: {{$i->humidity}}
@endforeach
```

iv. Finally, the registration of the Routes for the application takes place and this is done by the RouteServiceProvider within the “web” middleware group.

Algorithm 23. Code for registration of Routes for the application.

```
<?php
use Illuminate\Support\Facades\Route;
Route::get('dashdata', 'Datafields@dashdata');
```

This HTTP implementation does not make use of the broker.

8.3.2 MQTT

For the MQTT protocol implementation the mosquito PHP broker library was used. Moreover, the following command was used to install all repositories, packages, and dependencies for the MQTT communication model. Further information for the integration with the framework can be found in various sources over the web.

Command for MQTT installation via the composer

```
composer require salmanzafar/laravel-mqtt
```

Furthermore, the next command was executed to publish the MQTT service provider configuration file.

Command for Ponte IoT Framework installation

```
php artisan vendor:publish --
provider="Salman\Mqtt\MqttServiceProvider"
```

The code for the publishing and subscribing methods is presented below.

Algorithm 24. Code for methods publishing & subscribing.

```
<?php
namespace App\Http\Controllers;
use Illuminate\Http\Request;
use App\Datatable;
use Mqtt;
class Datafields extends Controller {
   function output() {
     $output = Datatable::all();
     return view('dashboard',
         ['output'=>$output]);
     }
   public function SendMsgViaMqtt($topic, $message){
      $output = Mqtt::ConnectAndPublish($topic, $message);
      if ($output === true) {
         return true;
      } return false;
   }
```

```
    public function SubscribetoTopic($topic) {
Mqtt::ConnectAndSubscribe($topic, function($topic, $msg){
          echo "Msg Received: \n";
          echo "Topic: {$topic}\n\n";
          echo "\t$msg\n\n";
       });
   }
}
```

The IoT framework used to develop the API provides reduced development time, reduced apparent complexity of deploying and operating an IoT network, improved application portability and interoperability, and improved serviceability, reliability, and maintainability.

8.3.3 CoAP

The code for the use of CoAP in the client side can be observed in algorithm 25 below.

Algorithm 25. Client structure for CoAP.

```
Create loop
Client – CoAP loop
Client – GET method and function (data) { decoding JSON data}
End_loop
Run()
```

The code for the use of CoAP in the server side can be observed in algorithm 26 below.

Algorithm 26. Server structure for CoAP.

```
Create loop
Server – CoAP loop
Server – Receive at ip_address and port_number
Server – On – Request function (request, resources, handler) {
          Resources = setPayload function {encoding JSON data}
          Send Data via the handler
End_loop
Run()
```

8.3.4 AMQP

The code for embedding and using AMQP inside a framework can be observed in the following algorithm 26.

Algorithm 27. AMQP publishing and subscribing.

```
Publishing and Queuing
AMQP publish key and msg
Queuing the name
```

Consuming
AMQP consume
function(msg + resolve message to body + msg ACK)

8.3.5 XMPP

The code for embedding and using XMPP inside a framework can be observed in algorithm 26 below.

Algorithm 28. XMPP communication.

Client Connection
Make a new client with options or connect manually

Sending Data
Fetch list of users or other groups
Setting a flag for the online status
Creating a new msg
Set msg and setTo (email)
Send msg
Create a new presence for email set, username, password
Send presence
Send msg
Disconnect

Chapter 9

Energy Efficiency

9.1 Overview

Battery life is one of the most important aspects that must be considered and tested during IoT development, system programming, and application development. The dissatisfaction of users, the decreased battery life, and the increased cost are some of the results of avoiding measuring the energy consumption of a system, platform or application. To measure the energy consumption of an application there is suitable software to do so. But measuring the energy of IoT platforms is more complex.

Hardware measurements can be done in Arduino with the use of the INA219 breakout board which has precision 1%. Software measurements can be achieved in the Visual Studio Code (https://code.visualstudio.com/) with the use of Platform IO extension (https://platformio.org/), which is a professional collaborative tool for development on embedded devices such as Arduino and sensing devices. Some of the functions and characteristics of this platform have been the fact that it is a cross-platform and unified debugger, it can analyze static code and test it remotely, it can also inspect the memory through specific firmware.

Another useful tool embedded in the "Cooja Emulator" running on the "Contiki OS" (https://www.contiki-ng.org/ or https://github.com/contiki-os/contiki), which runs on Ubuntu respectively, is the "Power Tracker" (Kaur and Matheshwari, 2016). With this tool the percentage of power used by every node in the network separately and the average power used by all nodes can be calculated.
All aforementioned will be discussed and presented in the next chapters 11 and 12.

9.2 Related Works

Xiaolin Fang et al. proposed an energy harvesting system with capacitor in order to supply energy in different timestamps. Researchers divided this issue into two different issues and proposed relevant algorithms. The first one is when there is not enough energy to deliver all data and the "offline" algorithm that has been proposed sends as more data as possible. The second one is when there is enough power to deliver all data and both algorithms try to reduce the time of completion. (Xiaolin Fang et al., 2018) Then, researchers proposed a low-power implementation of the protocol CoAP using the Contiki OS. Using a multi-hop network, it is shown that low power consumption at a higher latency cost is the result of using a duty cycle. (Pandesswaran C. et al., 2016)

M. V. Moreno et al. have been presented an energy saving solution in buildings with the aim to generate predictive models of energy consumption in buildings. Moreover, the authors have used a reference building, for which they have one year's coherent data, in order to verify the proposed solution. At the end, the authors propose strategies and control actions for energy saving in the building. (M. V. Moreno et al., 2016)

Chapter 10

Security and Privacy

10.1 Overview

Cyber-Crime is not different at all than regular crime that is all over the world from the past centuries. It is very important to recognize that we cannot stamp out the cyber-crime, as we cannot exterminate the typical crime.

However, there are two primary points to defend against cyber-attacks. The first point refers to the basic level of protection that companies and individuals can do in a daily basis, just like when you lock the door when you leave the house. It is important to secure the devices and the data the same way and use security principals, such as those used when protecting a person or a property. The second point refers to the deterrence. Today, there is a broad difference in laws and legislations. Many countries do not have vigorous cyber-security laws or are outdated and need to be modernized. In fact, having inclusive laws to operate as deterrent and well-read and well-trained personnel (judges, prosecutors, etc.) to persecute criminals when identified is an important aspect that plays vital role in fighting cyber-crime.

Many researchers claim that instead of using a simple password to secure data, devices, and systems there can be used modern security suites (e.g. G-suite), data loss prevention and encryption technologies, multi-factor authentication, and even, it can be done a system update on a daily basis to prevent the biggest percent of the attacks that occur.

James Dempsey (Executive director in the University of California – Berkeley Center of Law and Technology) once said in an interview: “Encryption is foundational”. What that means is that there is strong, default encryption and encryption with a government access option. He also said that building in government “backdoors” or access points as they can be characterized, means that vulnerability is created at the same moment.

The security model, which is used until now, is based on notifications and acquiescence. This means that first you are asked in most of the cases a question and then you have to agree or disagree by clicking “Accept” or “Decline” respectively (Wei Zhou et al., 2018). But now with the “Internet of Things” (IoT) devices, services, and systems are interconnected with each other and with the Internet, resulting in massive production of data that this model cannot withstand. This is because the collection of these enormous amounts of data is due to the millions of devices used in a daily basis (Sedrati and Mezrioui, 2018).

So, new privacy and security mechanisms should be implemented that will not use the notifications and acquiescence security model, but will take into consideration the limits of data collection and usage, the individual access and control of BD, and ways that up until now just have not existed. (Wencheng Sun et al., 2018; Jun Zhou et al., 2017)

"Artificial Intelligence" (AI) is a technological advance that provides various solutions to various issues, which are based on the security and privacy of data, by taking into consideration the energy consumption and the complexity of the algorithms.

To address the cyber-security threats, it is also important to make and have partnerships. This means that all information collected about security issues has to be shared in order to deploy better security mechanisms. So, it has to be a "shared responsibility" between the companies, the governments, and the citizens. (Wheelus and Zhu, 2020; Fahad Mira, 2019; Rachit et al., 2021; Wissam Abbass et al., 2018)

Last but not least, new legislations have been passed and more information can be shared between companies, governments, and citizens. But what information should be shared, what is most useful, in what context, and for who. These questions have to be answered by taking into account the impact on privacy which has to be in the lowest level.

As the amounts of data are produced by every device all over the world, there is an imperative need for data processing, data storage, data mining, data analysis, and of course data privacy. Data privacy is the most crucial issue since the beginning of the internet (20 years ago), as data production increases every day. Due to this, there have to be deployed strict rules and laws to secure the everyday amounts of data that are continuously raising fast. Such rules and laws had been introduced in the last 20 years. But 20 years ago, it was a very different era in terms of the Internet since it was not commonly used and it was not as much personally used.

Today, every European citizen has to follow the "General Data Protection Regulation" (GDPR) that came on for the "European Union" (EU). This is by far the most significant piece of European data protection enactment as Edina Bakos (Program Manager of Google Cloud) said.

10.2 Information Technology Service Management

"Information Technology Service Management" (ITSM) is a new rule for any business worldwide. It provides plenty of services, automates everything connected to the internet. More accurately, it provides data collection, data mining (extracting the information of data), data storage (cloud servers), data management, and data analysis capabilities/techniques and drive efficiencies in businesses. It increases the velocity of the delivered data. It also increases the "Quality of Service" (QoS). (A. P. Plageras et al., 2017)

Moreover, the ITSM gives solutions to problems faster so that it can increase the QoS and minimize the costs. Maybe the most important benefit that an ITSM can offer is the preventing and predicting capabilities to issues before they impact end users. (A. P. Plageras et al., 2017)

Everyone deserves great experiences in life. Now everyday tasks are done quickly with the use of complex services, systems, and standards. The criticalness of the "Information Technology" (IT) systems and services that a modern enterprise offers to its employees, subsidiaries or customers has led to the development of a set of best

practices called ITSM and includes factors such as maintaining a level of desirable operation, maintenance of IT infrastructures, their upgrading and their overall management since they have been shown to affect in many ways the operating costs and the reputation of the company.

Internationally established best practices concentrated in the "Information Technology Infrastructure Library" (ITIL) and the "International Organization for Standardization" or ISO (20000) standard to ensure the following results:

- standards of quality for IT services provided in agreement with suppliers and customers (internal and external)
- full monitoring of the quality level of the services provided and its imprinting in periodic reports through specific indicators
- organizing the gathering of service users' requests and ensuring a systematic and timely response to incidents and problems on the basis of predefined procedures
- organizational knowledge of troubleshooting and event management is organized to be used to resolve them more quickly
- monitoring changes in problem-solving and monitoring their impact on all IT infrastructures,
- monitoring the availability of services and checking the adequacy of infrastructure to meet the needs of users
- a comprehensive list of infrastructures is prepared to plan and monitor their changes and upgrades
- improving relationship with suppliers to maximize benefits and control costs
- assess and address the risks associated with the security of the traffic information
- computer-related expenditure is budgeted and monitored on an ongoing basis
- assess and improve the satisfaction of service users

In few words, it can be highlighted that there are several ITSM software platforms that provide automations, security (through the right ISO standard), and service management to companies and organizations. It contains various modular applications that are different at every user and every instance. The main purpose is to fix bugs, to provide security and notifications, and to automate every possible service.

The way this works is simple. First of all, the provider and the customer are setting up an agreement. This agreement includes all necessary parameters, standards, and the specific incidents needed by the customer. After the final agreement, the ITIL employees install the appropriate infrastructure. Then, all needed is an Internet connection since the platforms are usually cloud-based. "Cloud-based" means that the platform resides on the Internet and not on a local computer.

10.3 Related Works

Many researchers have proposed an IoT-based security framework on smart building scenarios. By this, they are integrating coherent data as fundamental components. The aim of the integration is to drive the building management and security behavior of indoor services accordingly. A holistic platform named City Explorer, which provides security and discovery, is the component in which the proposed framework is manifested. (J. L. Hernandez-Ramos et al., 2015)

The aim of another research is to provide a comprehensive review about smart cities. In addition, this research describes the IoT-based technologies used in smart cities. At the end, there have been explained practical experiences over the world and the main challenges such as those related with privacy issues of the citizens. (H. Arasteh et al., 2016)

A novel intrusion detection algorithm has also been proposed. This algorithm is based on sampling with “Least Square Support Vector Machine” (LS-SVM). Also, Enamul Kabir et al. in order to prove how effective is the algorithm proposed, they carried out experiments on a standard database, namely KDD 99 which is a "de facto" benchmark for the evaluation. (Enamul Kabir et al., 2017)

“Named Data Networking” (NDN) is used by a new secure data-centric “Building Management System” (BMS) architecture that has been proposed by Shang, W., et al.. Researchers also provide information to simplify user authentication and to control the access to data. Specifically, the BMS consists of end users, a gateway which is responsible for the insertion of data into the NDN-repositories so it can respond to users’ requests and provide security for “Distributed Denial of Service” (DDOS) attacks and other capabilities, and a manager application which is responsible for the management and the auto-configuration of the gateway. The NDN uses a data-centric model, which is responsible for the encryption of sensor data packets with a symmetric key which is sent to every authorized user. This model enables the appropriate connectivity and reduces the access to data in the authorized users. Also, as a keystone for the network communications, a novel Internet architecture proposed. (Wentao Shang et al., 2014)

Furthermore, for the security and the privacy threats, researchers proposed an ARM-compliant IoT security framework to be used in IB. This framework was established in a platform called City Explorer. Also, researchers expand the platform with safety mechanisms. (Jose L. Hernandez-Ramos et al., 2015)

Even though, S. M. Riazul Islam et al. proposed an intelligent collaborative security model. With this model, they want to minimize the security risks. Researchers also talked about the convergence of the new technologies, such as big data, wearable devices, etc., and presented the open issues and challenges on IoT-based healthcare systems. (S. M. Riazul Islam et al., 2015)

As applications based on IoT have been used widespread in every sector, many research studies provide useful information about new trends of IoT, the issues that they cause, some solutions that already exist, and various challenges that need to be solved in order to gain the benefits of the Internet technology.

Specifically, many researchers make illustrations of the most recent affection of issues based on security mechanisms, techniques, and methods related to the technology of the IoT. One feature of IoT that has a big impact on security and privacy of information is the interdependency. This means that due to the rapid increase of devices and data, more and more automation systems have been developed to make human interaction disappear. (Wei Zhou et al., 2018)

Nowadays, many of these systems are absolutely controlled by services, platforms, and applications such as the "Google Cloud", the "IoT Platform", and the "Android Applications" respectively. To sum up, the interdependence of devices, applications, and systems could be easily damaged by the attackers to fulfill their goals. Such a trigger that an attacker could have been the network level security, which in most cases is vulnerable at attacks like these related to DDoS attacks.

Moreover, another feature of IoT that is critical for the security of the automation systems is the variety of protocols used by the miscellaneous devices. For example, every device itself has a processor and its own characteristics, but cannot withstand every kind of protocol or feature that is out of its capabilities. (Wei Zhou et al., 2018)

A circumstance relevant to what just mentioned is the constrained energy of the IoT devices which constitutes the next feature of IoT. Due to the fact that these devices are very tiny and very lightly built, they do not need much energy to operate. This constrained energy leads to crucial problems and in most cases to vulnerabilities, because of the restricted security mechanisms and algorithms used.

Furthermore, networks of private computers, regularly named as "botnets", had been contaminated in the near past, with malicious software and were controlled as a group without the providers' knowledge. An example could be a spam message that was sent through the application to the user's device or more likely the DDoS attacks used by crackers to simulate users' requests and achieve their goal. (Wei Zhou et al., 2018)

In the past, many researchers had proposed detection systems and methods that detect DDoS attacks in devices which use the "IPv6 over Low-power Wireless Personal Area Network" (6LoWPAN) protocol (Wheelus and Zhu, 2020; Fahad Mira, 2019; Rachit et al., 2021; Wissam Abbass et al., 2018). In table 5 below, some of the most crucial threats in every IoT layer that have been studied by many scientists and some solutions can be observed. (Wheelus and Zhu, 2020; Fahad Mira, 2019)

Table 5. Crucial Threats in each IoT Layer

Layers	**Threats, Attacks, Vulnerabilities**	**Solutions**
Physical and Abstraction Layer	Unauthorized access to topics Tracking Denial of Service Repudiation Spoofing Packet Manipulation Eavesdropping DoS Exhaustion Unfairness Sybil	Authentication Knowledge security (RSA, DSA, Blowfish, DES, 3DES, etc) Access Control (Digital Signatures, MAC)
Network and	Unauthorized access	Authentication

Transportation Layer	Sybil attack Depression attack Sleep deprivation attack DoS Code injection attack Man-in-the-Middle attack	Secure Routing Knowledge Security Intrusion Detection Risk Management Risk Assessment
Application and Presentation Layer	Code injection attack DoS Spear-phishing attack Sniffing attack	Authentication Secure Routing Knowledge Security Intrusion Detection Risk Management Risk Assessment

The security mechanisms have to be updated and become even more adaptable to the changes that are coming together with the advances in technologies and the "Fifth Generation" (5G) of cellular networks. The 5G connectivity will bring new critical issues in security. (Wei Zhou, 2018 and Jun Zhou, 2017)

In table 6 below, the solutions for attacks that have been recorded in IoT environments have been presented and could be integrated in the proposed model.

Table 6. Solutions for Attacks & Problems in IoT Environments

Ref.	Attacks	Solutions
(Wei Zhou et al., 2018)	IoT botnets	1) Fuzzy rule interpolation (FRI) for detection, 2) Logistic regression which allows probability estimation, 3) Machine Learning techniques for IoT security threats detection 4) Auto-encoders 5) Adaptive filters
(Jun Zhou et al., 2017)	Physically dynamic tracing attack	Pseudonyms technique – hiding location and user identity,
	Node compromise attack and Target-oriented compromise attack	1) Authentication of users and devices/nodes, 2) Cloud-based IoT DTNs (Delay-Tolerant Networks) - credit-based incentive mechanism
	Injection attack	Avoid replication of victim node
	Layer adding attack Layer removing attack	Secure outsourced data aggregation without public key homomorphic encryption
(Fahad Mira, 2019)	Remote attack	Secure the area and devices
	Modification	Collision-free one-way hash function to guarantee the integrity of the message transmission

	Eavesdropping	Securing Key exchange process
(Wissam Abbass et al., 2018)	DDoS attack	1) Fuzzy rule interpolation (FRI) for detection, 2) Logistic regression which allows probability estimation, 3) Machine Learning techniques for IoT security threats detection 4) Auto-encoders 5) Adaptive filters 6) Lightweight agents – Blockchain smart contract
	Man in the middle attack	Non SSL and Secure connection SSL approaches
	Proximity-based attack	When combining large RSS-variation and matching between RSS-trace and smartphone sensor-trace to reliably detect and authenticate
(Nuzhat Khan et al., 2017)	Interception problem	Encryption of data
	Spoofing problem	Message Authentication Codes (M.A.C.) & Digital Signature
	Falsification problem	Message Authentication Codes (M.A.C.) & Digital Signature
	Repudiation problem	Digital Signature

The security algorithms mostly used in IoT environments are the symmetric and asymmetric encryption algorithms. (Lin Shi et al., 2021; Lv and Qiao, 2021; Taher M. Ghazal, 2021)

Block ciphers and stream ciphers are two encryption approaches related to the symmetric key cipher. They are applied in order to transform the plain text into cipher text. The main variation between them is that the former conducts the conversion through taking the block of plain text at once, while the latter conducts the conversion through processing 1 byte of plain text during each iteration. (Qing Fan et al., 2021; Khalid Haseeb et al., 2021; Maha Alqallaf, 2021; Shancang Li et al., 2021)

For the encryption and decryption in symmetric cryptography an identical key is used for both methods. Due to a comparative analysis of such algorithms used in IoT environments, some of the most known and used algorithms include AES (Advanced Encryption Standard), Blowfish, 3DES (Data Encryption Standard), Serpent, and Twofish. Symmetric algorithms are extensively used in data transmission and storage. However, it is not always easy or possible to share one secret key. (Nuzhat Khan et al., 2017; Dr. Sam Rizvi et al., 2011; Rana M Pir, 2016; Mishra and Acharya, 2021)

Asymmetric encryption is also known as public key cryptography. Its objective is to bypass the need to share one secret. The main idea behind this approach is to use different keys in encryption and decryption. Its base lies on problems that the designer thinks that are not solved fast such as prime factorization, discrete Logarithm, and

elliptic curves. After comparing such algorithms, the most known algorithms include ECDH (Elliptic-curve Diffie–Hellman), ECDSA (Elliptic Curve Digital Signature Algorithm), RSA (Rivest–Shamir–Adleman), El-Gamal, and SRP (Secure Remote Password). This type of encryption achieves data confidentiality (during the encryption phase), data integrity and authenticity (signatures) or key exchange over insecure channels. (Rana M Pir, 2016; Mishra and Acharya, 2021; Hassan and Hoomod, 2021; Mohammed Nazeh Abdul Wahid et al., 2018)

One common example of asymmetric encryption is the exchange of a message between Alice and Bob. Alice and Bob generate a pair of keys (public and private). The public key has been published over the internet. The encryption of the message has been performed using the public key of Bob by Alice, and transmits it to Bob. The decryption of the message has been performed by Bob using his private key in order to decrypt the messages that have been encrypted through the public key. Also, Alice uses her private key in order to sign a message, and transmit it to Bob. Bob verifies the integrity and authenticity of this message, since he knows the public key of Alice.

Moreover, the problem of a number factorization has gained significant attention in modern cryptography as several cryptographic protocols base their safety in the difficulty of solving it (with the most known and applied the RSA). The RSA cryptosystem was proposed by Rivest, Shamir and Adleman and is the first public key-based cryptosystem. (Rana M Pir, 2016)

Furthermore, Chaotic encryption is based on the mathematic chaos theory. Some of its main applications are image encryption, aimed at improving the security of digital images, generation of hash functions, and generation of random numbers. There are both symmetric and asymmetric chaotic cryptographic algorithms, however the majority of the relevant approaches falls under the asymmetric group. Furthermore, discrete chaotic maps are commonly used in relevant applications.

AES has been proven robust against all major security attacks. Its cipher key is consisted of at least 128 bits, which provides 2128 possible keys. Hence, the conduction of brute force attack is impractical. Furthermore, this algorithm applies an S-box substitution table that is retrieved through the determination of the multiplicative inverse for a given number in Galois field, being capable of resisting both linear and differential cryptanalysis. However, it is vulnerable to timing attack, since the applied sequence of S-box lookups takes variable time and depends to the key. (Dr. Sam Rizvi et al., 2011; Mohammed Nazeh Abdul Wahid et al., 2018)

On the other hand, RSA is vulnerable to brute force attack, since it applies a short secret key. Furthermore, RSA can be broken under mathematical attacks that exploit the mathematical properties of the algorithm, based on prime factors. Increasing the length of key is considered as a countermeasure against this vulnerability. An acceptable size of modulus is 2048 bits. (Rana M Pir, 2016; Mohammed Nazeh Abdul Wahid et al., 2018)

Furthermore, RSA is vulnerable to timing attack, since the attacker is able to exploit the timing variation of the modular exponentiation or determine d through the necessary time for the computation of $C^d \pmod n$ for a cipher text C. There are several

counteractions about these vulnerabilities (a constant exponentiation time for all exponentiations, a random delay to the exponentiation or the multiplication of the cipher text with a random number. (Rana M Pir, 2016; Mohammed Nazeh Abdul Wahid et al., 2018)

Finally, another vulnerability of RSA lies to the chosen ciphertext attack. The product of two cipher texts is equal to the encryption of the product of the respective plaintexts, setting easy for an attacker to conduct a relevant attack. This issue can be resolved through padding a random number to the plaintext.

As for speed, AES provides higher speed, albeit this feature is decreased when using constant time in order to resolve the vulnerability of timing attack. On the other hand, RSA is more functional. Therefore, a combination of the two algorithms is the most suitable approach. RSA, based on asymmetric cryptography, can be used to authenticate the parties and agree on a key for a symmetric system. Then, AES, based on the symmetric approach, can be applied for large data blocks in order to take advantage of its higher speed.

To replace DES, the Blowfish algorithm is a 64-bit block cipher with a variable-length key mechanism (Data Encryption Standard). Blowfish also separates a message into 64-bit chunks of equal size. There are two aspects to the algorithm: key expansion and data encryption. Blowfish is faster than DES in terms of encryption time; nonetheless, the algorithm's weak point is its weak key. There is currently no cryptographic attack capable of breaking the Blowfish algorithm in an acceptable length of time. System weaknesses are most likely to blame for the attack's success. Anyone can use Blowfish because it isn't patented or requires a license. CAST (Carlisle Adams & Stafford Tvares) uses a 128- or 256-bit key format, similar to the DES algorithm. (Dr. Sam Rizvi et al., 2011)

The Twofish algorithm is a symmetrical block technique that uses 128-bit blocks and 256-bit keys in cryptography. This algorithm is linked to the Blowfish algorithm before it. Pre-calculated key-dependent S-blocks and a complex encryption mechanism are the two primary aspects of the Twofish algorithm. One-half of the n-bit encryption keys is used to encrypt data, while the other half is used to alter the method. (Dr. Sam Rizvi et al., 2011)

The architecture of the Twofish algorithm is similar to that of the Blowfish technique. In terms of speed, Twofish may be able to outrun AES. On a range of CPUs and platforms, Twofish is fast and adaptable. Twofish is suitable for network applications where keys are frequently updated, as well as where RAM and ROM are limited. (Dr. Sam Rizvi et al., 2011)

The advantages of the blowfish algorithm include its speed and efficiency, as well as its ability to generate big, secure keys. The Blowfish Algorithm can grow and develop a larger and longer length, boosting the speed with which computer systems handle data while maintaining system security. (Mohammed Nazeh Abdul Wahid et al., 2018; Dr. Sam Rizvi, 2011)

Vernam’s One-Time Pad is a stream cipher that functions by applying the boolean operation XOR (as described in 1st semester’s “Introduction to Computer

Science") to the plaintext. It offers "perfect secrecy" but is otherwise impractical when one needs to encrypt large streams of data.

Data Encryption Standard (DES). One of the oldest block ciphers (since 1977), which was used by governments, banks and finance companies. It uses a 56-bit key to encrypt 64-bit blocks of data in 16 rounds, by applying mathematical permutations, substitutions and other functions. DES is not in use any more, due to its low security.

An advanced version of it is 3DES ("triple DES"), which is technically DES applied three times to each data block. This process renders it more secure, although slower than DES, which has contributed to 3DES being used until today.

Chapter 11

Proposed Convergence of Technologies and Solutions

In this chapter, the most relevant solutions and scenarios proposed by the author of this dissertation have been listed. These solutions and scenarios have been evaluated since they have been published in the proceedings of international journals, conferences, workshops, and magazines, and have been strongly peer-reviewed.

11.1 Proposition 1

The following architecture has been proposed regarding the work: ***"Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings"*** that has been published in the proceeding of the "Future Generation Computer Systems" journal (2018).

Concerning the related work studied and the comparative analysis made, it has been designed and simulated a topology-architecture system for a smart building, in order to offer an energy efficient solution by using the collected and managed sensors' data.

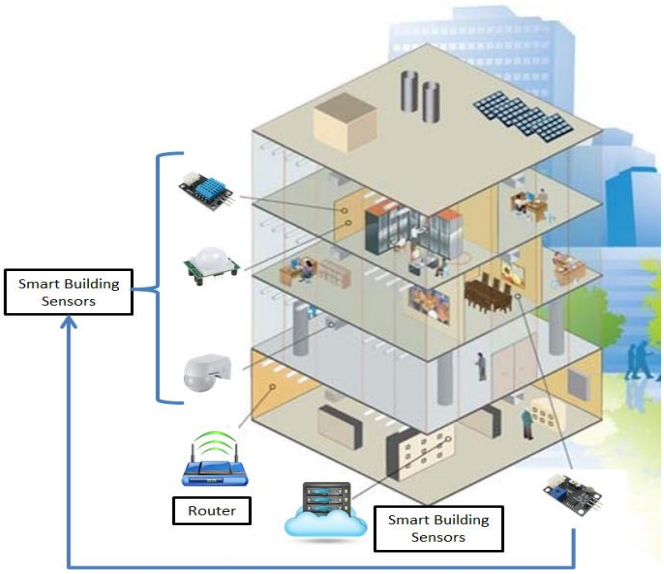


Figure 17: Smart building components.

Based on figure 17, it has been implemented a system that includes sensors that take measures for temperature, movement, light and moisture with the aim to achieve a better management of the building and also, to make the building smart and efficient. As it can be observed in figure 18, in the low level of the building, there has been a cloud server that helped in the building's management and storage of the valid information from sensors.

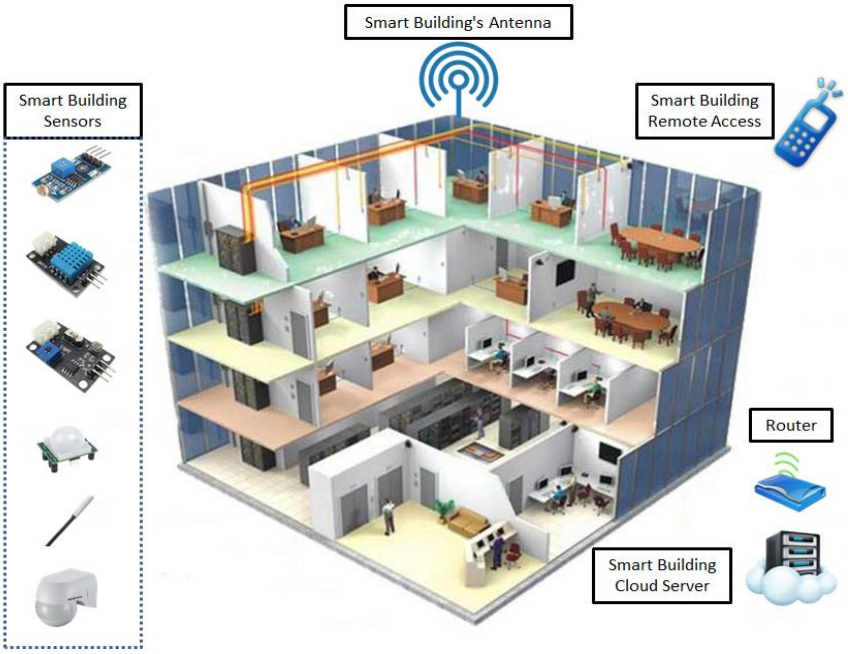


Figure 18: Smart building connection.

More specifically, in figure 18 it can be seen the communications between the various sensors that can be installed in the building and the cloud server with the users. Users have had remote access to sensors' data, and also, they could manage the information of the data in order to be able to make some actions. For example, through the remote access a user could receive a signal that there is a high temperature with the aim to activate the air conditioning before going home. Additionally, using the analyzed, from the cloud server, measurements which were recorded by the motion sensor, the user will be able to understand if there is someone in the house, which can offer "security" sense.

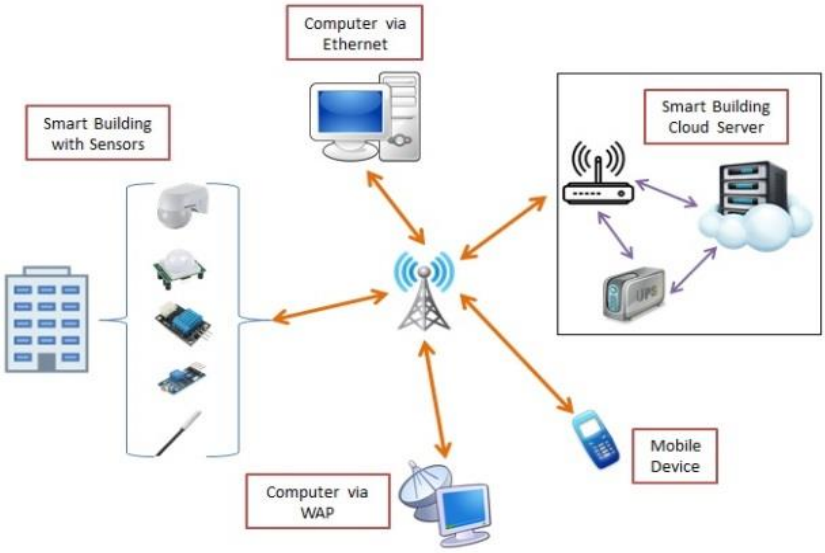


Figure 19: Proposed Architecture.

Figure 19, demonstrates the architecture of the proposed system, and the logic of communications between the user, the sensors, and the whole smart building. The topology of the network has been hybrid, relaying on star and mesh topologies. This could offer a reliable network, easy to be managed in error detecting and troubleshooting. The mesh topology which already is and will be more popular in the future provides many benefits. One of these benefits is the tolerance that it has in errors. The star topology, which is widely used in home networks, provides also fault tolerance but since the middle connection point is working properly.

Also, the installed cloud server could operate autonomously by using a voltage stabilizer (UPS) to avoid any problem. All the users could easily connect to the network through the Wi-Fi connection of the building and remotely through their mobile providers. The installed network has been supporting the communication protocol IPv6 and a "Network Adaptive Multisensory Real-time Transmission Protocol" (NAMRTP) proposed in previous work. This protocol can transmit from the remote environment to the database real-time multisensory data in a reliable way.

Simulations carried out using an operating system investigated by A. Dunkel and which is called Contiki and can be found as "*Instant Contiki 2.7*" (I. Romdahani et al., 2016). In Figure 20, it has been presented the proposed simulation using the Contiki Operating System (OS) and its applications to simulate the network and extract from the network nodes measurements for the data collected and transmitted. Also, these data can be stored in specific files for analysis at future time. The Contiki OS is open-source and was designed for small and smart devices which are not expensive and provide low power consumption. Also, it is used for the collection of the large amount of data. Furthermore, Contiki Simulator has been used instead of the lack of hardware resources. For the simulation of the network in real-time it has been used the Cooja emulator.

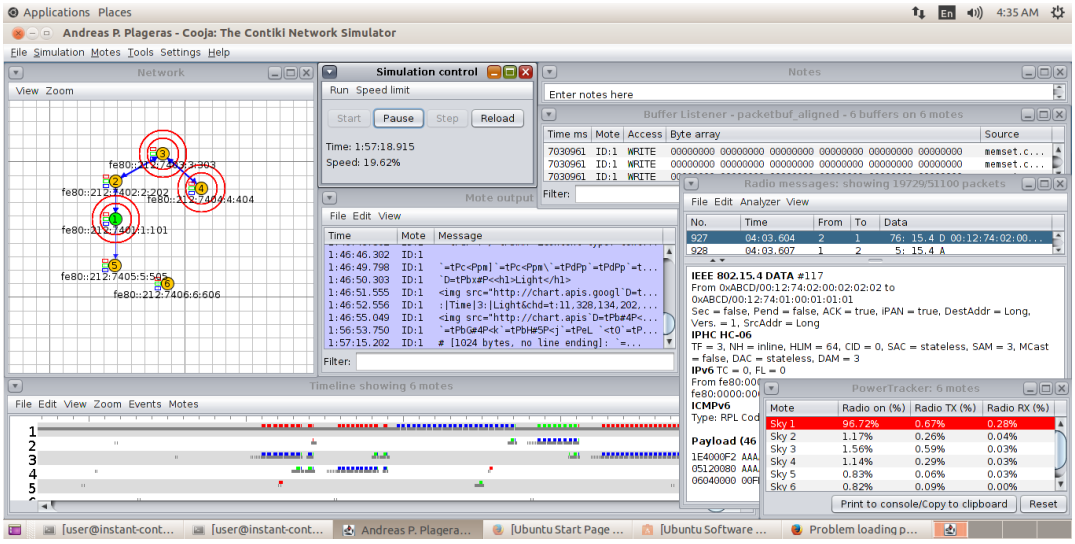


Figure 20: Simulating with Cooja emulator of the Contiki OS.

The new simulation is shown in Figure 20 above, where there are several windows. The one on the left-up corner is the "Network" window where it can be seen the network topology. From this window every node in the network can also be accessed so that it can be configured to take measurements. The second window is the "Simulation Control" window from where the simulation can be "started", "paused", made a "step" forward, and "reloaded". The window on the top-right corner is where notes can be taken, and that is why it has been named "Notes" window. The window in the middle called "Mote output" is where are printed for each node all outputs of serial ports. The last window observed when a New Simulation has been created, is the "Timeline" window. There, are shown the packets of data delivered over time.

Since the "IPv6 over Low-power Personal Area Network" (6LoWPAN) has been built and shown in Figure 20 above, more tools can be used such as the "*Radio Messages*" tool from the menu "*Tools*". In the "*Radio Messages*" window, it has been chosen the "*6LoWPAN Analyzer with PCAP*" from the menu "*Analyzer*". With that choice made and after the simulation has started, the network traffic (data packets) has been saved in a "*PCAP*" file for future analysis.

Another useful tool is the "*Power Tracker*" which can be found in the menu "*Tools*" with the name "*Mote radio duty cycle*" (Kaur and Matheshwari, 2016). With this tool the percentage of power used by every node in the network separately and the average power used by all nodes can be calculated. These measurements can be observed in table 7 below.

Table 7. The power of each node in different states.

Motes	Radio on (%)	Radio TX (%)	Radio RX (%)
Sky Mote 1 (Border Router)	96.72%	0.67%	0.28%
Sky Mote 2	1.17%	0.26%	0.04%
Sky Mote 3	1.56%	0.59%	0.03%
Sky Mote 4	1.14%	0.29%	0.03%
Sky Mote 5	0.83%	0.06%	0.03%
Sky Mote 6	0.82%	0.09%	0.00%
AVERAGE	17.20%	0.35%	0.03%

Specifically, there have been collected information about the power used by each node and the average power of all nodes and the power used during the processes of transmission (TX) and receiving (RX) of data packets for each node and for the average of all nodes.

Then, the proposed network has been built by inserting nodes in the Network window. We just need to go to the menu "*Motes*" and select the appropriate type. In this case, the "*Sky mote*" type has been used, which provides 8 MHz MSP430 low power microcontroller, 10 KB RAM, and 48 KB flash memory. This type of nodes also provide 250 Kbps, 2.4 GHz, IEEE 802.15.4, "*Chipcon Wireless Transceiver*" and sensors that take measurements of humidity, temperature, and light, 16-pin expansion support and

optional SMA antenna connector. It has also been used the "*Sky mote*" type, because they can all support the 6LoWPAN.

But, why 6LoWPAN has been chosen? This type of network has been chosen because it is basically an IPv6 duplicated version, so that the IPv6 can work with low-power radio frequency at the physical layer. And why it is required the IPv6? It is required because by that way, IoT devices communicate over the Internet separately one at a time. Firstly, a border router has been added.

Moreover, more sensor nodes of type "*Sky Mote*" have been added in the network. There have also been chosen to add the program "*sky-websense.c*". This application has been used to produce sensor data and to give access to the most recent data. This happens through a web server who is converged in the application. So, it has been a need to add some sensor nodes in the network, in order to collect the data produced by them. After starting the simulation the blank windows have been filled with information as demonstrated in Figure 20.

Specifically, in the "*Radio Messages*" window, if a click has been made on a message it could obtain precious information, for example, it can be found out if IPv6 has been used. In addition, a program named "*tunslip6*" has been used in order to connect the router with Cooja.

The experimental results from the simulation run on Cooja have been demonstrated below. The simulation is ready to start, and a ping can be executed in a new terminal for any address which belongs to a node in the network. The results have been presented in Figure 21, where from the "*ttl*" and the "*time (ms)*" the hops of each node from the router are noticeable. More accurately, the border router has ttl=64, the node which is one hop away has ttl=63, the node which is two hops away has ttl=62, and so on. That can be observed in the next Figure 21. The same can be observed with the transmission time which is lower at the nearest to the router hops.

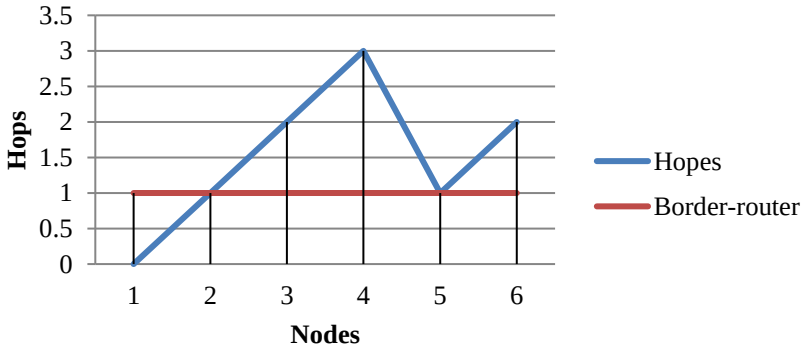


Figure 21. Hops per node from the Border Router.

With the ping that was executed are also provided information about the duration of transmission and the packet loss which is described by the following Equation (1):

$$TDS = TDR + PL \qquad (1)$$

where TDS, TDR, and PL represent the total data sent, the total data received, and the packet loss respectively.

As already mentioned, information has been provided about the protocols used for the communications between the nodes, for example, the IEEE 802.15.4, the IPv6, the 6LoWPAN, the CoAP, and so on. Moreover, by opening a browser (e.g. Firefox) and typing the IPv6 address of the border router, it prints as output the neighbors and the routes. By typing the IPv6 address of any other node, there are printed the temperature and the light. The temperature that has been shown in Figure 22 is same and stable for all nodes. This could be described by the following Equation (2):

$$TT = T1 = T2 = T3 = T4 = T5 = T6 \qquad (2)$$

where TT is the Total Temperature and T1 to T6 are the temperatures of nodes 1 to 6.

The data collected by these light-sensors has been represented for each node in Figures 23, 24, 25, 26, and 27 respectively.

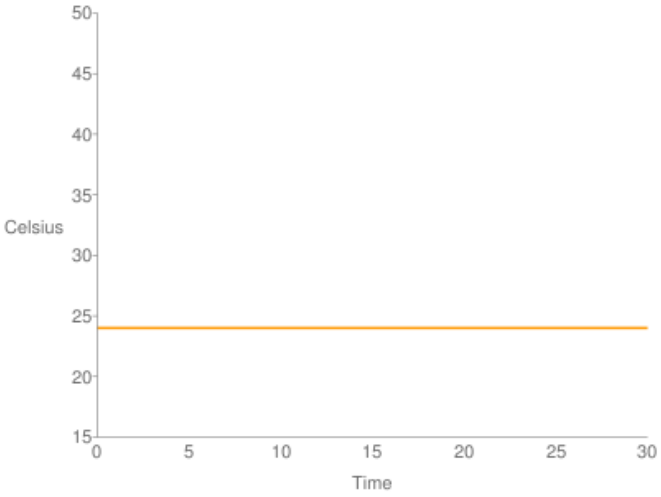


Figure 22. Temperature in all nodes.

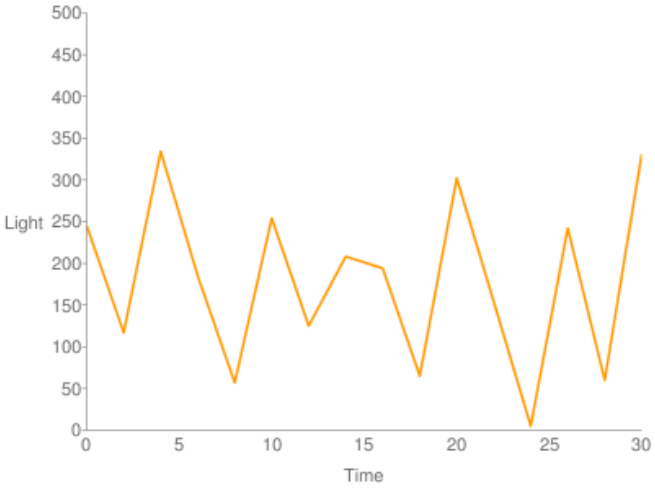


Figure 23. Light in Node 2.

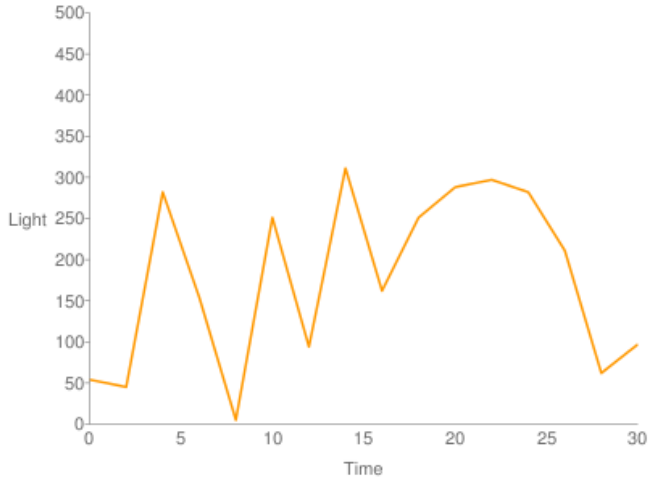


Figure 24. Light in Node 3.

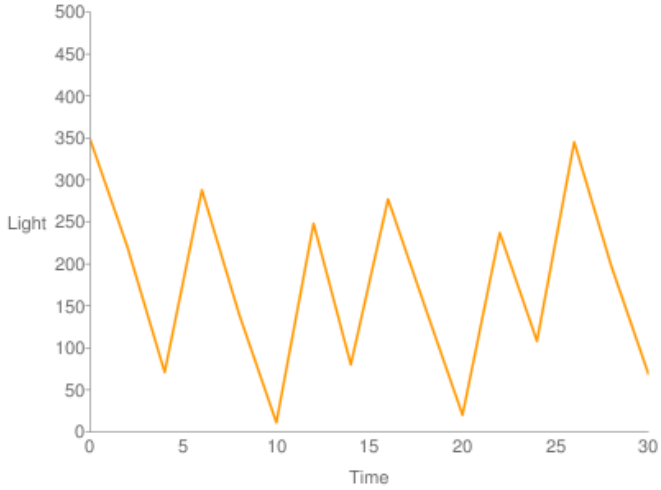


Figure 25. Light in Node 4.

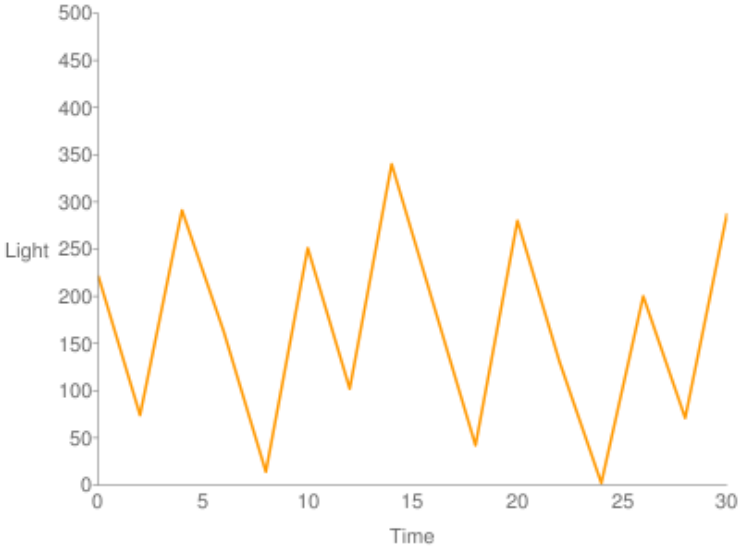


Figure 26. Light in Node 5.

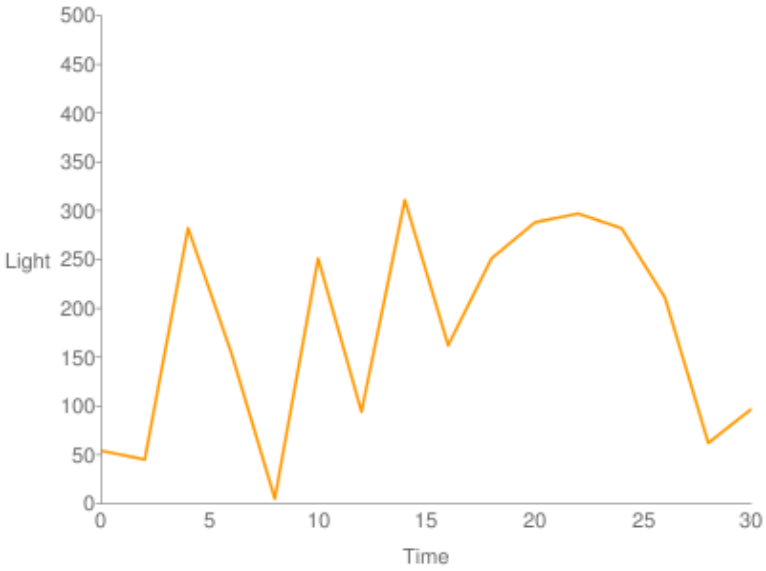


Figure 27. Light in Node 6.

After the simulation has been stopped, open Wireshark and then, open the "*.pcap"* file created. As already mentioned, this file contains all packets transmitted. So, using Wireshark there can be observed information about the communications. In the following Figure 28 the situation described above has been presented.

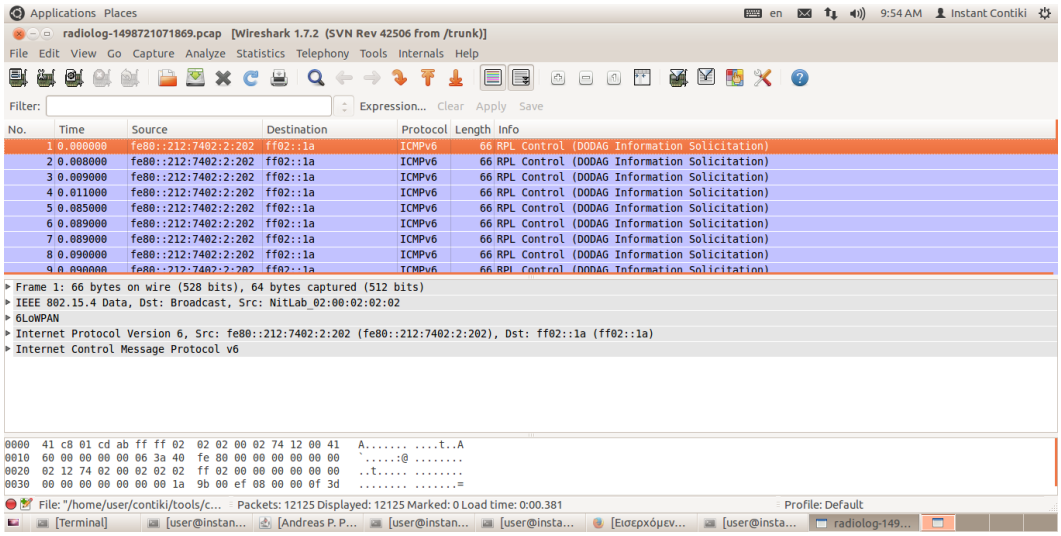


Figure 28. Using pcap files in Wireshark.

With the proposed system it can achieved energy efficiency, with the use of the collected and managed sensors' data. In contrast with previous works, it has been implemented a system that includes sensors that took measures for temperature, movement, light, and moisture with the aim to achieve a better management of the building and also make the building "smart" and efficient. In the proposed system, users would have remote access to sensors' data and also, they could manage the information of the data in order to be able to make some actions. Furthermore, with the use of the

analyzed data (measurements which were recorded by the motion sensor) users will be able to understand if there is someone in the house, which can offer "security" sense.

New and better solutions for making Smart Cities more efficient implanted and presented by the technologies surveyed in this research work. Cost reduction, safer environment, comfortable and friendly applications could be achieved through a system which can exploit all the abilities of the technologies studied. With multiple sensors installed in a Smart Building it can be achieved a better monitoring system for the whole building. The proposed systems implemented in a simulation environment of Cooja Contiki.

This work surveyed IoT, CC, BD, and sensor technologies with the aim to find their common operations and combine them. Moreover, regarding smart city concept, it has been tried to propose new methods in order to collect and manage sensors' data in a smart building, which operates in IoT environment. Finally, the proposed solutions for collecting and managing sensors' data in a smart building could lead in an energy efficient smart building, and thus in a "Green Smart Building".

11.2 Proposition 2

The following architecture has been proposed regarding the work: ***"Efficient Large-Scale Medical Data (eHealth Big Data) Analytics in Internet of Things"*** that has been published in the proceeding of 19th IEEE International Conference on Business Informatics (CBI'17), International Workshop on the Internet of Things and Smart Services (ITSS2017).

The aim of this research is the collection of medical (e-health) large-scale data (Big Data) in real time, by sensor devices (sensors) and actuators (actuators), which will be worn on patients (wearable devices) who suffer from chronic or rare or hereditary diseases. The collected data have then been transported (in real time) through the network to a cloud server, and subsequently have been processed in the CC, which makes the analysis to mine knowledge from these IoT data, which have no significance if they are not analyzed. Finally, the transfer (in real time) of the analyzed health data has been held into the devices (smartphones, tablets, PDAs, laptops, and so on) of the relevant persons (doctors, caregivers, other family members, etc.) to address problems in the health sector (D. Tomtsis et al., 2015; G. Kokkonis et al., 2016; S. Kontogiannis et al., 2016; Stergiou and Psannis, 2016).

Contrary to the practices used to date, pervasive data came to "stay", and to improve health care, with more accurate diagnoses, with shorter delays for the patient's treatment, and with fewer obstacles for patients when making treatment. (Andreas P. Plageras et al., 2016)

In this research, given the challenges which are growing in the healthcare sector, it has been proposed a system shown in Figure 29, which provides to the relevant people and in real time, via sensors and other devices, medical information related to the health of a patient, so as to monitor the state of health out of the hospital, freeing thereby

places (such as a hospital bed) and resources of the hospital (such as food), and further savings and provide more comfortable environment for the patient.

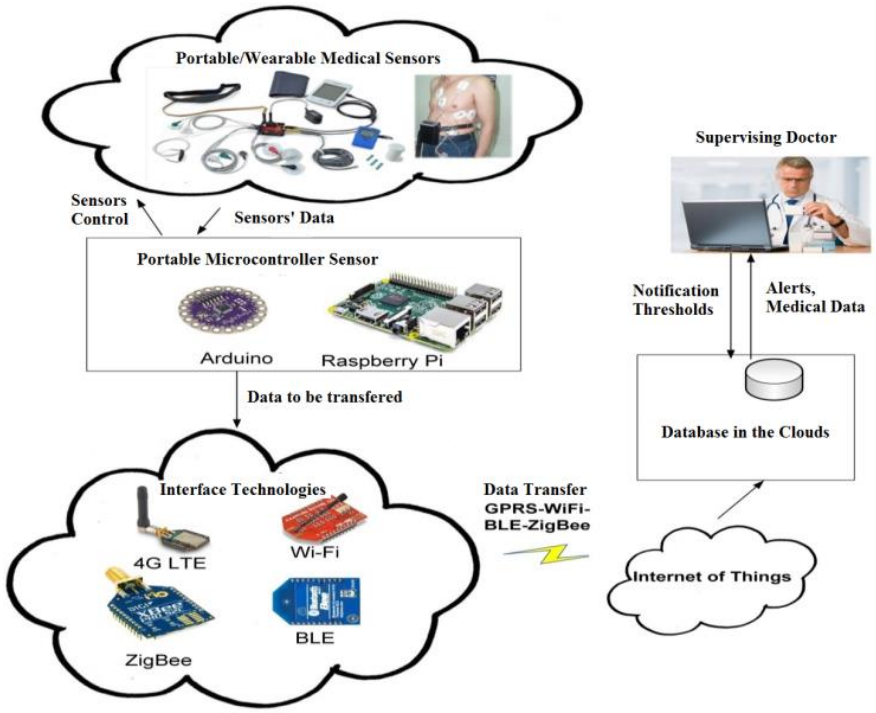


Figure 29: "The architecture of the proposed system".

At the same time, in this way, it has been accomplished the direct information of the patient for the state of his/her health, the timely information of the doctor-nurse about the state of health of the patient, the remote patient monitoring, the timely information of medical personnel for emergencies in order to correctly and quickly prepare for an emergency, the direct conversation of the patient and the doctor so that there is no distortion of information by playing the "broken telephone", as well as, the better organization records of physicians so that the information will not be altered with the passage of time. (Andreas P. Plageras et al., 2016; G. Kokkonis et al., 2016; S. Kontogiannis et al., 2016; D. Tomtsis et al., 2015)

So, in addition to improve healthcare for patients, this research proposal aims to address the challenges of these technologies, and to the creation of a system which has been advantageous over the systems that have been proposed by other researchers. Tuan Nguyen Gia et al. have been presented the integrated architecture of their proposed system in which they use the "IPv6 over Low-power Wireless Personal Area Network" (6LoWPAN) technology, which is scalable and has fault tolerance, so that the sensor nodes maintain the connection between them.

Moreover, Anurag et al. have been presented a "pervasive healthcare system» ("an IoT-based pervasive healthcare system"), which gives patients a normal life without qualified medical staff to monitor their health, accurate medical data and an alarm system for emergencies. The two systems that have been applied in this

investigation for the remote monitoring of patients are a wireless sensor network, which is based on low-power ZigBee technology, and a wireless sensor network, which is based on IP (Internet Protocol), and which uses Wi-Fi. (Tuan Nguyen Gia et al., 2015; Anurag et al., 2014)

The system that has been proposed takes precedence over these two systems, because of the combination of more wireless data transmission technologies, such as the technologies 6LoWPAN, ZigBee, Wi-Fi, LoRaWAN, and "Bluetooth Low Energy" (BLE).

As a final benefit of this research proposal has been the presentation of proposals to optimize the integrated use of BD technologies, IoT, and CC, particularly in terms of analysis of the management and medical content data networking levels.

In this research for testing and real time simulation and monitoring of the network and the conditions in it, there have been used many different tools. One of these has been the Contiki OS and the Cooja emulator. In Cooja emulator has been created a simulation scenario in order to test the entire system. This has been helpful in order to provide more realistic and detailed experimental results. In the following Figures (Figure 30-44), the Cooja environment can be observed.

Specifically, in Figure 30 has been shown the environment of the Cooja emulator. On startup some basic windows that have been opened can be observed. The first on the left is the "*network window*" where someone can build the network by adding and managing the network nodes.

The second window at the top-center of Figure 30 is the "*simulation control window*" that has four buttons (one for starting the simulation, one to pause it, one to stop it, and one to reload it). The third window is for "*notes*". The fourth window is the "*mote output window*" where the output of the nodes has been shown. Finally, the fifth and last window is the "*timeline window*" where the packets per seconds can be observed.

Moreover, in Figure 31 the average temperature of the nodes (sensors) has been presented and in Figure 32 the temperature of the sensors has been presented. Then, in Figure 33 has been shown the battery voltage of the sensors and Figure 34 shows the battery indicator. Furthermore, in Figure 35 and 36 are shown the relative humidity of the sensors and the latency of the network respectively. In Figure 37, the packets received into the network over time and in Figure 38 the packets lost over time can be observed. Also, in Figure 39, the packets received per node and in Figure 40, the hops per node have been presented.

Moreover, the average power consumption has been estimated in Figure 41 and the average radio duty cycle has been estimated in Figure 42. Finally, the instantaneous power consumption and the history of the power consumption can be observed in Figures 43 and 44 respectively.

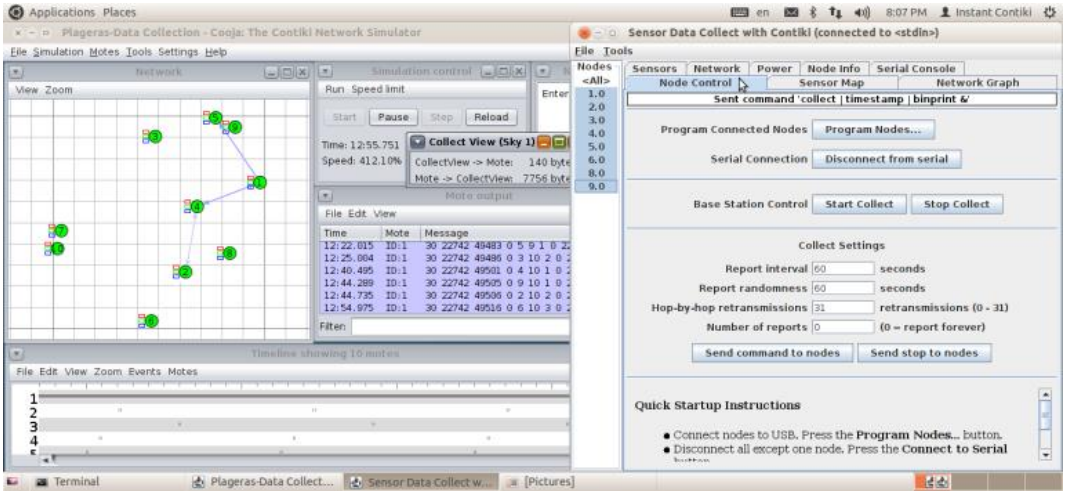


Figure 30. The Cooja Emulator.

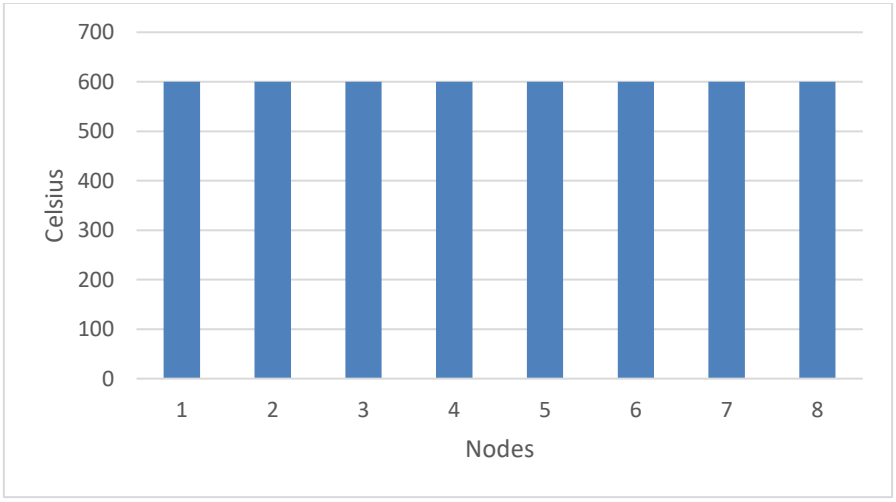


Figure 31. Sensors' Average Temperature.

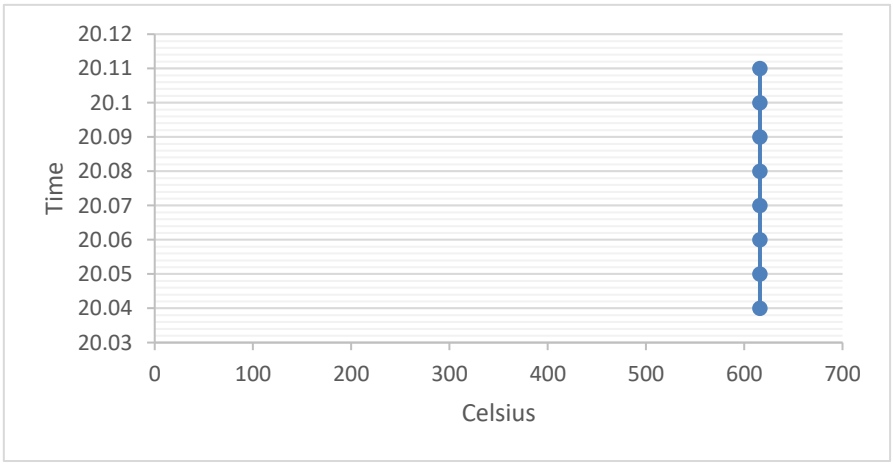


Figure 32. The Sensors' Temperature.

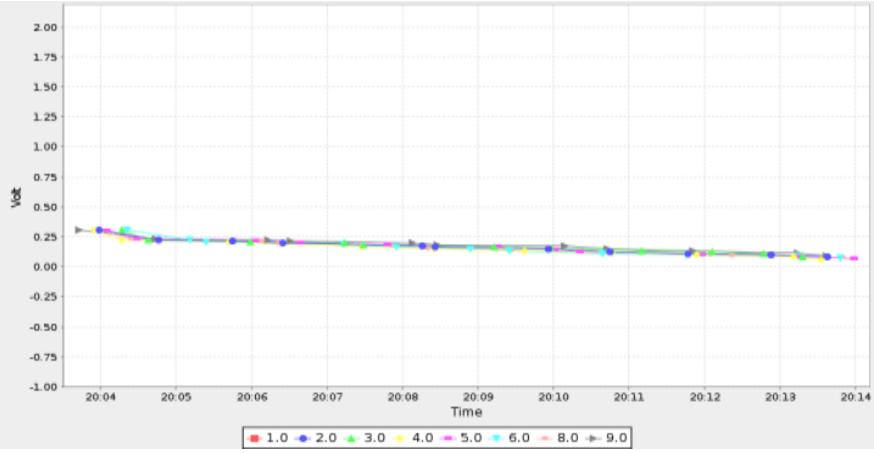


Figure 33. The Sensors' Battery Voltage.

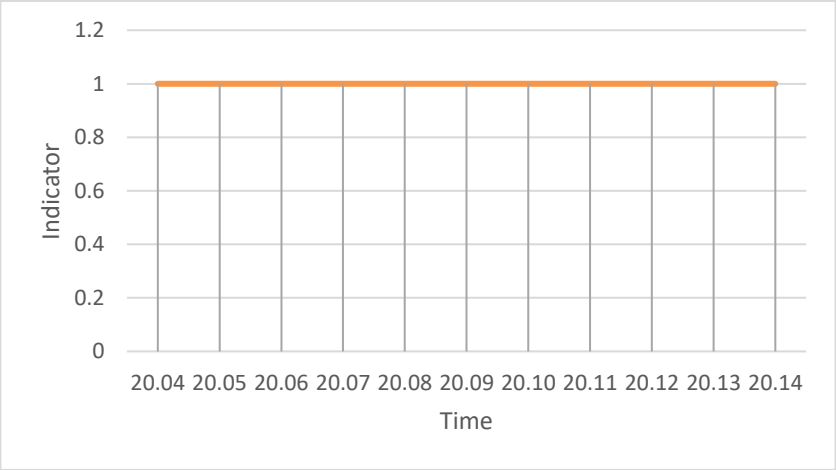


Figure 34. The Sensor' Battery Indicator.

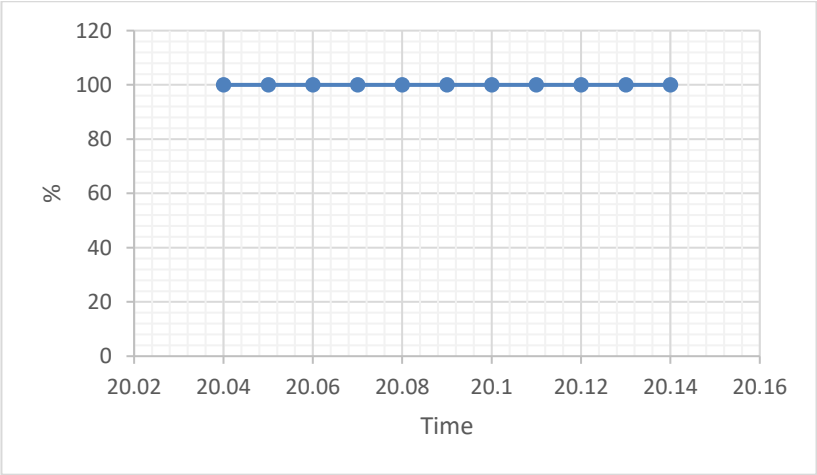


Figure 35. The Sensors' Relative Humidity.

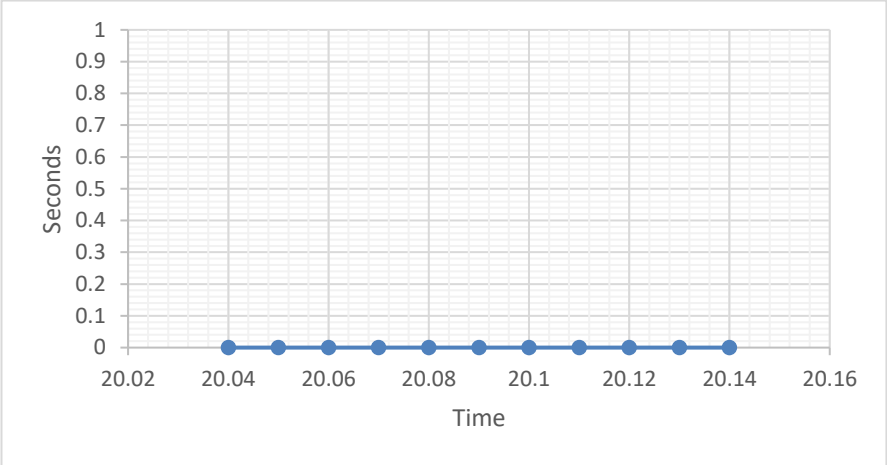


Figure 36. The Network's Latency.

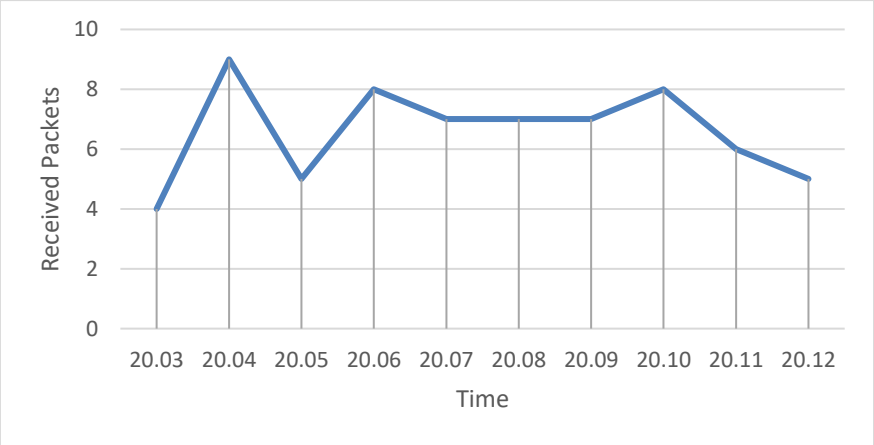


Figure 37. The Network's Packets Received (over time).

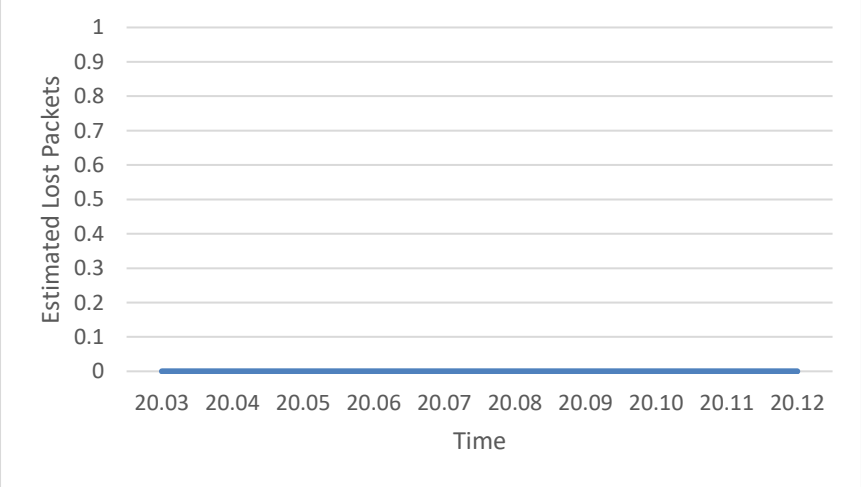


Figure 38. The Network's Packets Lost (over time).

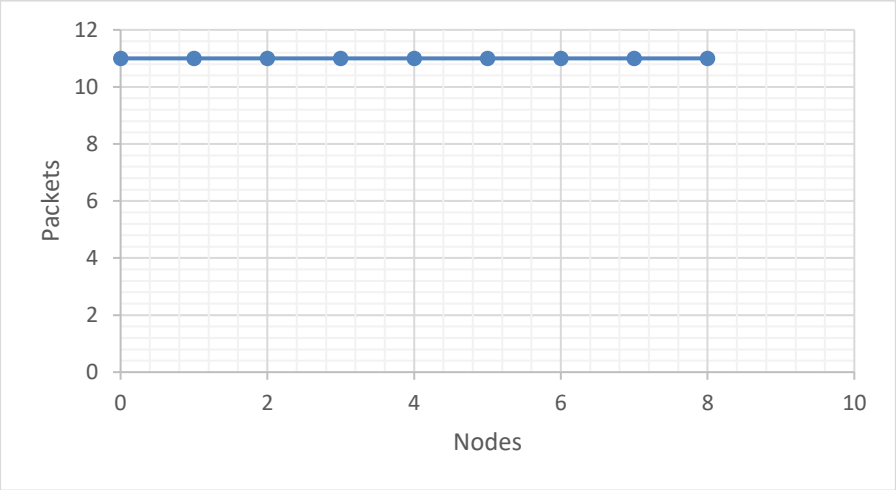


Figure 39. The Network's Packets Received per Node.

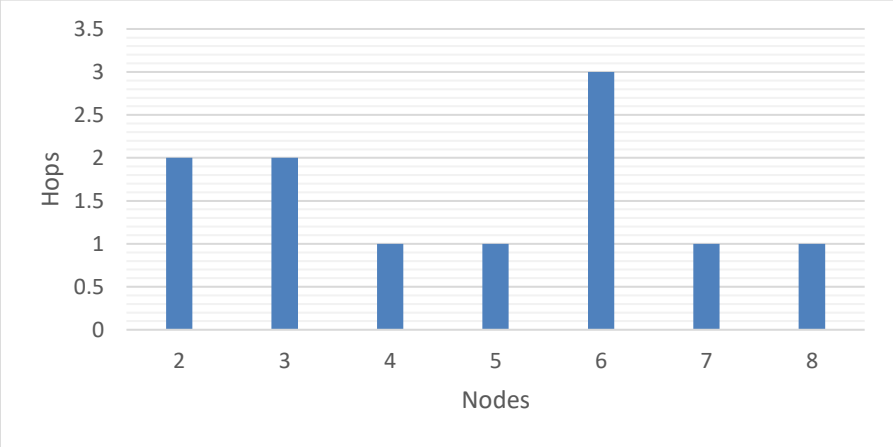


Figure 40. The Network's Hops per Node.

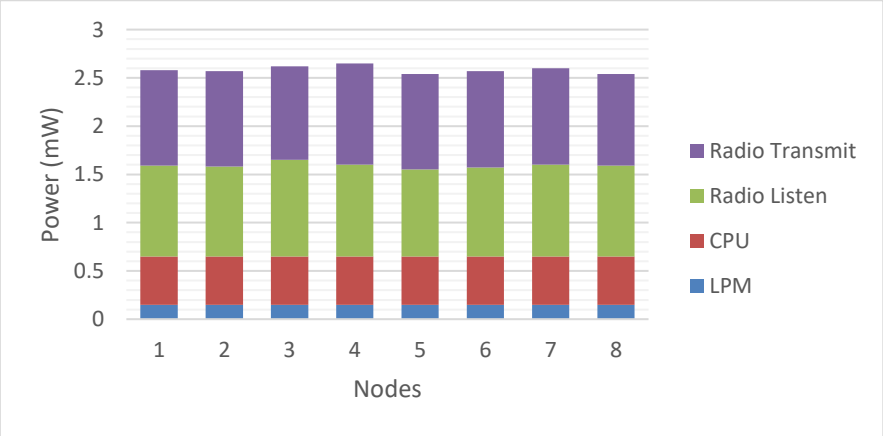


Figure 41. The Average Power Consumption.

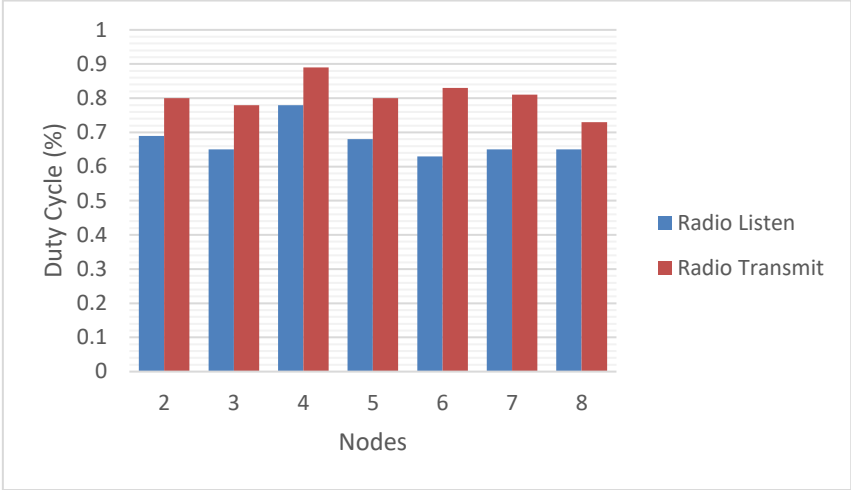


Figure 42. The Average Radio Duty Cycle.

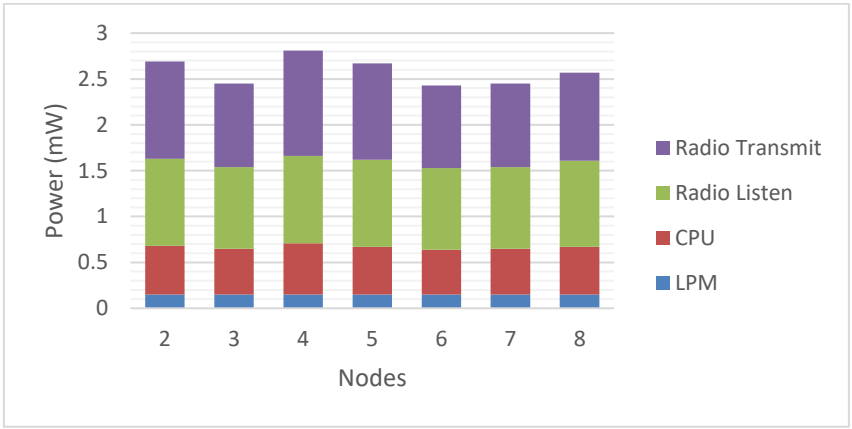


Figure 43. The Instantaneous Power Consumption.

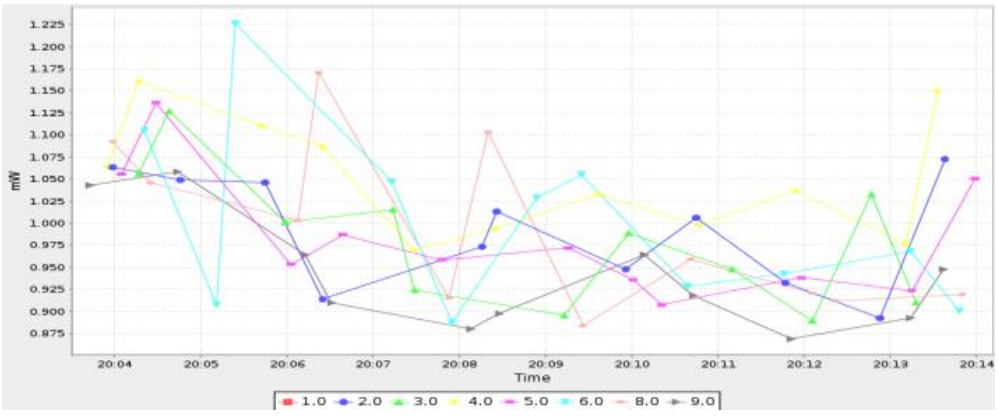


Figure 44. The History of the Power Consumption.

The results of this research contribute to theoretical and applied scientific knowledge. From the perspective of theoretical knowledge, a comparative analysis of data transport protocols for real time communications via the Internet has been performed and presented in the previous subsection. These protocols have been well

applied to different kind of sensors in the general scientific field of WSN. There have been proposed the best ways to protect the transmitted medical data.

It has also been investigated the smooth transition in real time of one wireless data transmission technology to another (e.g., Bluetooth Low Energy to LoRaWAN). Particular attention in this case is that there is no loss of data and the period of transition to be as soon as possible.

From the perspective of applied scientific knowledge, particular emphasis has been given to the "Hybrid Transmission Data System". The hybrid data transfer system combines the main and the modern technologies of wireless data transfer such as Wi-Fi 802.11ac, ZigBee, BLE, and LoRaWAN. Depending on the geographical topology of the system (distance and signal strength), the energy that feeds the sensors (battery status), the type of medical data (real time or not), and the amount of data shall be applied, in case of a different method of sending data, based on the above technology.

In case of adoption of a future expansion of this proposal in hospitals around the country will strengthen the economy of hospitals and mental health of patients. The not too sik patient would not need to be in an unfamiliar hospital only to monitor his/her health. All medical data will be recorded by sensors and then, will be sent in real time to the doctor on duty. By this way, the patient will feel comfortable in familiar surroundings and the Hospital will increase the available resources and beds will be released for more emerging situations.

Medical data will be collected by health sensors and will be sent to a medical research center, which already collaborate research fellows, for further study of the results.

This research focuses in the field of bio-informatics and IoT. The novelty of this research has been observed with the combination of these two regions. To transfer sensitive medical data, a hybrid wireless technology to send data, which takes account of all modern methods of wireless data dispatch, will be investigated. Also, new data transfer protocols that take into account the particularities of each wireless network protocol and optimally combine the latest wireless technology to send data need to be proposed. Methods for sending data, that could be included in this research are the ZigBee, the BLE, the LoRaWAN, the Wi-Fi 802.11ac, and the 4G/LTE.

If the patient is walking, a distance from the access point to the Internet and the energy of the sensor are not of important interest and the Wi-Fi 802.11ac protocol can used. If the sensors have limited power, the protocols BLE and ZigBee can be used with the help of a modified data transfer protocol that is based on the way in which processes the sensor data transfer protocol CoAP. If the patient is at distance greater than 50 meters and less than 2 km from the Internet access point, then the data will be sent to investigate if the LoRaWAN protocol can be used. If the patient is in an area not covered by these protocols 4G/LTE mobile network can be used.

Particular emphasis needs to be given about the security of medical data, which constitute personal data by applying innovative methods in their coding. It has been quite important for both the patient and the doctor to have the supervision to provide security in their communication and data exchange. Security can be based on

development and implementation of a communication protocol, which focuses on the secure transmission of medical data and provides encryption to them, with the help of encryption algorithms that can be processed (Andreas P. Plageras et al., 2016; Stergiou and Psannis, 2016; G. Kokkonis et al., 2012; G. Kokkonis et al., 2015).

The maximum upload rate in each protocol according to the distance needs to be provided. Which of the medical data can be sent in real time and which with time delay? A smooth transition way can be offered by the one wireless technology to the other, while minimizing delays and packet losses. Data compression algorithms have been proposed to reduce the sending rate, especially, when the network has been congested. Also, further research for the quality assurance of the data dispatch service must be done. Then, the maximum data security in the hybrid wireless data network can be ensured.

Regarding the analysis and management issue of the large-scale data in the health sector, a new type of technology could be used in order to help. The main objective of this research proposal has been an analytical study of the technologies IoT, CC, and BD with the aim to resolve the various issues that have been faced in the sector, in relation to these technologies. The main purpose of this research proposal has been at first the collection of medical (e-health) BD in real time. The collection performed by sensor devices and actuators, which have been worn on patients who suffer from various ailments (e.g., chronic, hereditary, and rare diseases).

Subsequently, takes place the transfer of these data through a network to a cloud server. Furthermore, these data have been processed in the cloud, and then have been analyzed in order to gain some meaning for the user. By the analysis of these data takes place the data mining procedure. Finally, the transfer of the medical data that have already been analyzed has been provided by the devices that have been worn by specific people, in order to address the various health problems. Also, this study deals with the security of these medical data, which constitute personal data, and must be protected. For this reason, in the next sub-section, there have been applied innovative methods in their coding regarding their security.

11.3 Proposition 3

The following architecture has been proposed regarding the work: ***"Solutions for Inter-connectivity and Security in a Smart Hospital Building"*** that has been published in the proceeding of 15th IEEE International Conference on Industrial Informatics (INDIN'2017).

Since various technologies, communication protocols, security mechanisms, and interconnectivity challenges of plenty of research have been studied, a theoretically-based contribution of interconnectivity and security in intelligent buildings has been presented. Specifically, a theoretically-based design of an Intelligent Hospital System has been presented. The purpose has been to propose a new architecture, to secure the sensitive health data and the whole hospital, and interconnect every system and object (device) in the building.

Firstly, a solution for the energy efficiency of a smart building can be observed, since it is the major problem of applying complex security mechanisms for the safety and the security of patients. Also, this solution improves the process of all control systems in the building and makes the environment more comfortable. From the owners' side, it reduces costs and energy usage.

The solution for energy saving in the hospital, if it can be started from the very beginning of its construction, is the convergence of all the necessary parameters and systems for energy saving. Such parameters and systems are the wind generators, the hydroelectric generators, and the storage and use of solar energy. Thereafter, the energy gained by these physical ways must be stored, so, that it can be accessed and managed by the "Building Automation/Management System" (BAS/BMS). A BAS/BMS includes the smart lighting, the elevators, the cooling (HVAC), other electrical elements, physical security systems (fire, safety, etc.), and other smart building components. Such BMSs that are open source facilitate the IoT interoperability in intelligent buildings.

Because nowadays to construct a building from scratch is difficult enough, solutions for the already constructed buildings have been provided.

On the one hand, for the energy efficiency of a hospital, it has been decided that integrating smart grid with the hospital building is necessary for the energy usage management. A BMS will be the key component for the management of the energy and the actions of the building. In other words, the decisions will be taken from the BMS.

Figure 45 below, shows the layers of the proposed intelligent hospital BMS design. The design has three layers. The first layer (field layer) consists of sensors and other end devices and systems (e.g., smart grid) since in this layer takes place the integration of them. The second layer is the middleware. In this layer, the integration of the physical systems with the cyber systems is done. This layer is called automation layer. In the automation layer takes place the processing of the collected data, the execution of control loops, and the activation of every alarm in the building. The last layer is the efficient management layer. In this layer, the decisions and the aggregations take place, due to the knowledge of the building, the smart grid, and the condition and "covet of the tenants" (e.g., patients, doctors, managers, etc.). (Luca Catarinucci et al., 2015)

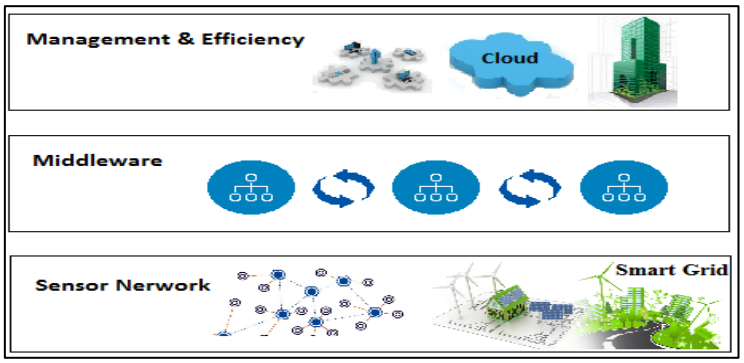


Figure 45. The layers of the intelligent hospital BMS design.

In a previous section, some security solutions for securing devices, data, and the whole building have been introduced. So, by the combination of these solutions with the benefits of IoT technologies and the architecture proposed in previous work, a secure intelligent hospital design has been proposed and presented in Figure 46. (Andreas P. Plageras et al., 2016)

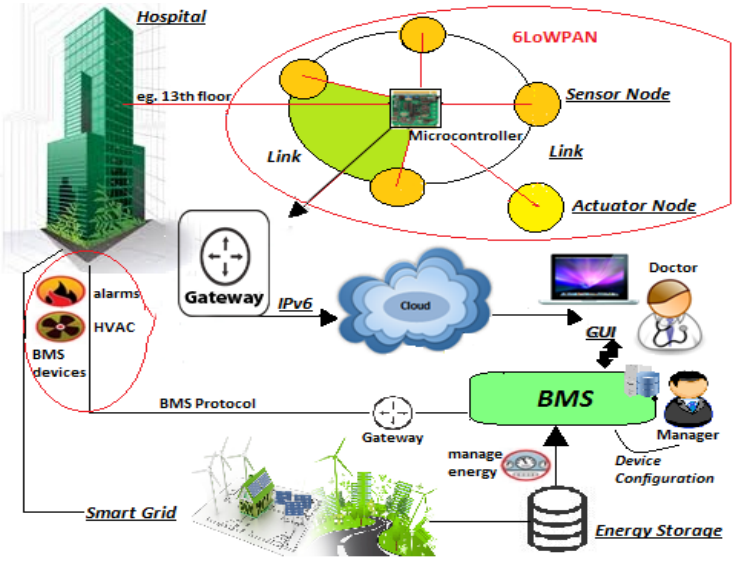


Figure 46. Intelligent hospital building design.

A hybrid network topology has been designed, which is a combination of star and mesh topology. In every floor and in every room, there have been installed sensor and actuator networks (6LoWPANs), which have been all connected to microcontrollers. Each microcontroller has been collecting the data from each node of the network, and then, the data has been sent through the IPv6 communication link to the gateway. The gateway consists of a local database and a router. Then, the router has been sending the data to the remote environment, which is namely the cloud platform. This platform consists of a database and a remote cloud server. In this database have been stored the data and then have been analyzed. The cloud server has been storing the real-time data and has been analyzing them. In addition, in the building, there have been parts like fire alarms, smoke detectors, etc., that can be combined with the stored energy and all the building's devices. Then, they can be efficiently managed by the BMS.

Describing the OSI layers of this design which have been shown in table 1 below, there is the IEEE 802.15.4 protocol at the first two layers (Physical and Data Link Layer). This protocol has been used to connect the devices and start the communications between them. The IEEE 802.15.4 standard has been providing low data rate, low power, and low-cost communication of devices that have been nearby and which have limited infrastructure. (Andreas P. Plageras et al., 2016)

The next layer is the data link layer, which consists of two sub-layers. The "Media Access Control" (MAC) sub-layer, which has been the IEEE 802.15.4 and the Adaptation sub-layer of the 6LoWPAN. The 6LoWPAN is a technology that has been

used for the header compression and encapsulation of IPv6 data packets so that they can be transmitted and received. This technology, also, has been providing high reliability, adaptability, energy efficiency, mobility, low cost, reduced overhead, and raise in the maximum possible payload.

Then, the IPv6 (6LoWPAN) protocol is used in the network layer, since it is the future of the Internet communications and the authentication of every object. The IPv6 protocol provides benefits that deal with low costs (equipment and infrastructure costs) and interoperability since it is enabled by the use of information technology (IT). In this layer has been taking place the addressing and the routing of data. (Wentao Shang et al., 2014)

The next layer is the transport layer, where the communications between devices' applications have been produced. In this layer, the protocol used in previous work is the "User Datagram Protocol" (UDP). This protocol is faster than "Transmission Control Protocol" (TCP) and supplies lower latency, but often has been used for audio and voice streaming applications (e.g., Skype, Viber, etc.). That is because if a UDP message is lost, it will not be re-sent automatically. For that reason, the TCP/IP protocol has been used for the communications. This protocol has been providing reliability of the sensitive health data by using a three-way handshake process. (Andreas P. Plageras et al., 2016)

In the last layer called application layer has been used the "Constrained Application Protocol" (CoAP), a Restful web application layer protocol. This protocol is mostly used for devices that are running on batteries and for devices that use energy harvesting. Benefits from the use of CoAP have been the low overhead and the IP multicasting. (Andreas P. Plageras et al., 2016)

Table 8 below, shows the OSI layers and the protocols used by the intelligent hospital system.

Table 8. The layers and the protocols used.

OSI Layers	Sub-layers	Protocols
Physical Layer	-	IEEE 802.15.4
Data Link Layer	MAC	IEEE 802.15.4
	Adaptation	6LoWPAN
Network Layer	-	6LoWPAN, IPv6
Transport Layer	-	TCP/IP
Application Layer	-	CoAP

Finally, there is the BMS architecture which uses a new Internet architecture called "Named Data Networking" (NDN). In NDN every IPv6 address is replaced with data names which consist of two data packet types (the Interest type and the data type). In these data packets are carried the requests and the responses. In each packet, there is also a signature for the authentication by the data consumers. Two benefits from the use of the NDN are the routing scalability and the long-term storage. By that fact, every object or even a whole system of objects identified in the hospital has a name despite an IP address. Such an NDN solution has been presented by Wentao Shang et al. (Wentao Shang et al., 2014)

Table 9 below shows a comparative analysis of the benefits of our proposed approach to other similar situations.

Table 9. The benefits of the proposed approach over two other similar.

Research Benefits	Proposed	Andreas Plageras et al. 2016	Luca Catarinucci et al., 2016	Georgios Lilis et al., 2016	Pandesswaran C. et al., 2016
Inter-connectivity	X	X	X	X	
Energy Efficiency	X	X	X	X	X
Reliability	X	X	X	X	X
Adaptability	X	X	X	X	X
Flexibility	X	X	X	X	
Scalability	X	X	X	X	
IPv6	X	X	X	X	
Security	X	X	X		X
NDN security	X				
TCP/IP	X				
CoAP	X	X	X		X
BMS	X			X	

Some of the benefits of the proposed approach have been the energy efficiency from the integration of smart grid, and the interoperability challenges provided. Also, the system has been characterized as adaptable, reliable, flexible, and secure. On the one hand secure because of the security mechanisms that have been provided in every layer, every floor, and every room in the proposed hospital building. On the other hand, secure from the point of view in which security services can be provided in the hospital for everything and everyone in the building. Every door, every service, even every object could also be equipped with fingerprint protection or even with face detection and recognition techniques, when and where the appropriate systems (fingerprint and camera systems) have been involved in the equipment of the building.

Since an overview of the proposed design has been done, solutions and ideas on how to secure the building could definitely be proposed. In the data link layer (adaptation sub-layer) there has been the 6LoWPAN. For the encryption and the authentication of the links, it has been provided the AES-128 link layer security. Secure data packet delivery and message delivery has been provided by the 6LoWPAN. In the network layer, there has been the IPv6 protocol. In the transport layer, it has been used the TCP which provides reliability to the data and "Transport Layer Security" (TLS) mechanisms. Using all these mechanisms, safer communications between the devices have been provided. Also, CoAP has been used in the application layer, which is responsible for the compression and the transmission of the sensitive health data. (Andreas P. Plageras et al., 2016)

NDN has also been used to secure the BMS. In the network layer for example, a signature in every packet and other optional encryption have been integrated.

With the use of Contiki OS and the Cooja emulator, there have been created simulations of the system in real time. These helped to have a more detailed and realistic image of the system.

There has been created an example simulation of the protocol CoAP which has been used for the transmission of data in the application layer. In the following Figure 47 have been presented the network nodes topology, the bytes of data (packets) transmitted, the packets lost during the transmission, the packets received, the time of that real-time simulation, the bridging between the nodes (servers) and the node (client) to the border-router, the requests, and responses of the network nodes, etc.

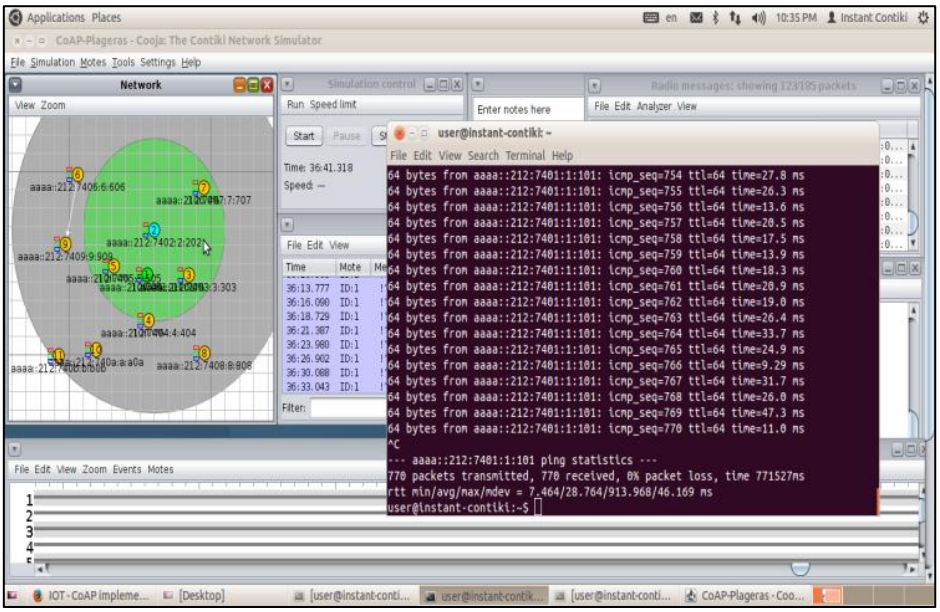


Figure 47. Simulating the transmission of data with CoAP.

Figure 48 shows the results from the ping of the IPv6 address of the router ("ping6 aaaa::212:7401:1:101").

```
64 bytes from aaaa::212:7401:1:101: icmp_seq=754 ttl=64 time=27.8 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=755 ttl=64 time=26.3 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=756 ttl=64 time=13.6 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=757 ttl=64 time=20.5 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=758 ttl=64 time=17.5 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=759 ttl=64 time=13.9 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=760 ttl=64 time=18.3 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=761 ttl=64 time=20.9 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=762 ttl=64 time=19.0 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=763 ttl=64 time=26.4 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=764 ttl=64 time=33.7 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=765 ttl=64 time=24.9 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=766 ttl=64 time=9.29 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=767 ttl=64 time=31.7 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=768 ttl=64 time=26.0 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=769 ttl=64 time=47.3 ms
64 bytes from aaaa::212:7401:1:101: icmp_seq=770 ttl=64 time=11.0 ms
^C
--- aaaa::212:7401:1:101 ping statistics ---
770 packets transmitted, 770 received, 0% packet loss, time 771527ms
rtt min/avg/max/mdev = 7.464/28.764/913.968/46.169 ms
user@instant-contiki:~$
```

Figure 48. Ping statistics of the router with IPv6: “aaaa::212:7402:2:202”

In the following figure 49, we read the sensors using the nodes' ipv6 addresses, by inputting in the Firefox browser, which uses cu plugin, the following address: "coap://[aaaa::212:7402:2:202]" (IPv6 of Node with ID:2) or any other sensor node's IPv6.

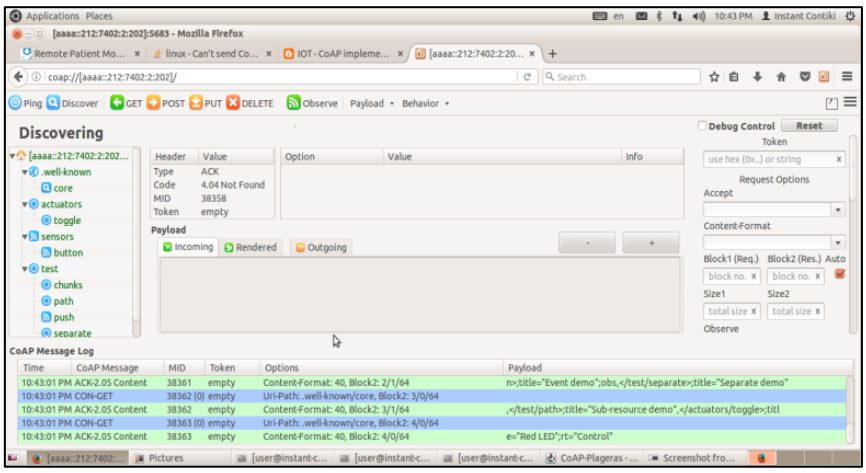


Figure 49. Reading the sensors with the use of their IPv6 addresses.

In this research, has been proposed an intelligent hospital building design. Solutions for the security and the interconnectivity of the building and the data produced have been presented. Specifically, the OSI layers of the proposed design have been analyzed and then, after research in every field have been presented some efficient security and interconnectivity solutions. Solutions for the energy efficiency of everything in the building, has also been reported in this paper. Finally, the Contiki OS and the Cooja emulator have been used to simulate parts of the system in order to have a more detailed and realistic view of the proposed architecture. From the results, it can be concluded that the architecture is interoperable and secure, but further research and experimentation is needed, in order to have an implemented idea.

11.4 Proposition 4

The following architecture has been proposed regarding the work: ***"Efficient Big Data Delivery over IoT networks"*** that has been published in the proceeding of the 4th World Symposium on Communication Engineering (WSCE 2021).

The most recent advances in the Internet of Things era demonstrate a new communication model. This communication model has three layers, namely the "Physical-Abstraction" layer, the "Networking-Transportation" layer, and the "Application-Presentation" layer. This model architecture has been presented in Figure 50 below.

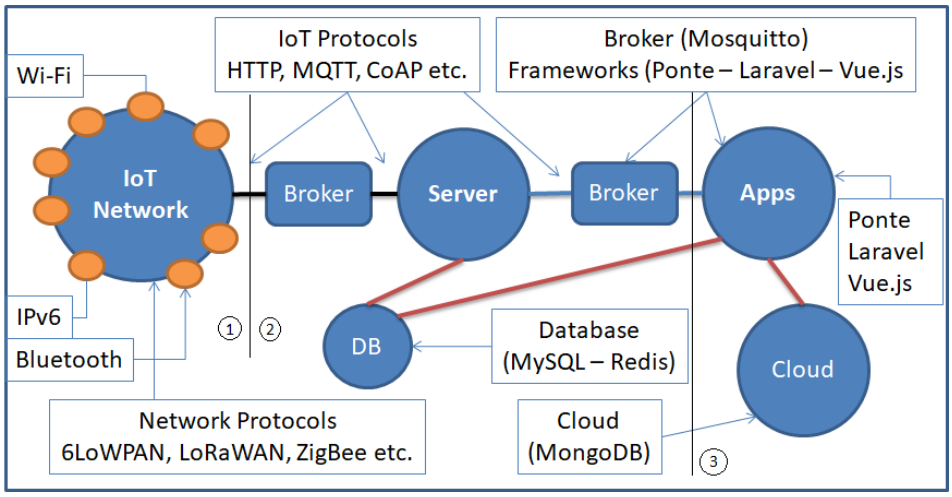


Figure 50. IoT model architecture.

In Figure 50, it can be observed the proposed IoT system which has been divided in three layers. The first layer got its name from the IoT-devices that are inter-connected in a way and topology so that they can produce data every second efficiently. These data are useless until suitable algorithms are developed and thus, knowledge is mind out of them. These algorithms will be integrated in the code-file for each sensing device. This file is stored in the server side and includes the database connection script, the device set-up script, and the efficient algorithm. The algorithm is an efficient loop which is different for every sensor and was made to fulfill the relevant needs. For example, a body temperature sensor will update the database field that holds the value of the temperature, only when a specific change of the temperature is detected. The code is uploaded to a microcontroller such as Arduino via the Sketch application (I. Heđi et al., 2017).

The second layer, which can be named as the middleware, consists of a database and a broker. The local database has a table with the appropriate columns and fields to store the collected values of each device. This table was migrated by the framework. The table will work in conjunction with the mining algorithm, so that the fields are updated with the new values in real-time via the broker (Elias Yaacoub et al., 2019).

The broker is software running on a device. It eliminates security issues in connections and vulnerabilities. It provides scalability from a single device to thousands of devices and manages all client connection states. Two devices can directly exchange messages (peer-to-peer). This is accomplished by sending a message to the broker, which then forwards to any device as a clone. This is namely the publish/subscribe model (Elias Yaacoub et al., 2019).

This model is efficient and provides safety in communications of devices and data exchange. The publisher, which can be any IoT device, transmits the data to the broker under a specified “topic”. Then the broker forwards this topic to any subscriber device that requests the specific topic. For example, in our case the temperature sensor publishes the temperature to the broker device under the topic “temp”. The specific topic that holds the data for the temperature will be available to any subscriber that asks for the temp topic. Each publisher is a different device/sensor that could be added in the system and publish a unique topic and each subscriber is the device that requests the specific topic. Thus, the broker is responsible for the transmission of the information stored in the database to the API (Application Programming Interface) in real-time. The

broker is also responsible for the transmission of the data collected to a cloud server for further analysis and complex monitoring.

In this layer, as a database and cache storage, have been used and tested the well-known MySQL database system and an open-source key-value storage called Redis. The Redis has the ability to store some data inside a key. These data are namely "a value". If the key is acquainted then the data stored in that key can be retrieved. As a result, "*Redis*" database acts as a broker. This database provides also high availability and automatic partitioning. The "*MongoDB*" could be also a very efficient solution since it is a NOSQL database (non-relational) and since it provides cloud services and insights.

The third layer (application layer) is where the Laravel PHP-framework has been used. This framework provides the DOM (Document Object Model) of the API (Charilaos Akasiadis et al., 2019; Emanuele Di Pascale et al., 2019). In simple words, it contains a structure for efficient application development and it is based on the MVC (Model-View-Controller) architecture (Annie Gilda Roselin et al., 2019; Mingqiang Zhu et al., 2017; Rakesh Kumar Lenka et al., 2019).

To start with the first layer, Mining Association Rules are considered to be one of the most important data mining processes. The rules of correlation provide a better understanding and user friendly way to analyze the potential information that could be characterized as useful. These rules reveal hidden "connections" between the features of a data set. These connections have been presented by researchers in the form $A \rightarrow B$, where A and B are sets that refer to the characteristics of the set of data analyzed. Given a set of data, an $A \rightarrow B$ correlation rule predicts the appearance of the characteristics of set B given the appearance of the characteristics of set A.

Moreover, the sensors produce a series of digital signals. These signals may hide some noise. Thus, the implementation of complex digital filters may not be desirable due to the complexity of the calculation and due to the relatively high energy consumption.

Simple smoothing may be enough to remove the noise. Exposure smoothing is one feature of the self-rotating moving medium model. Its output is derived from the current input value and the previous calculated value. The equation below describes the exposure smoothing feature.

$$O[\nu] = \alpha * I[\nu - 1] + (1 - \alpha)\, O[\nu - 1] \qquad (1)$$

O is the output value, *v* is the number of the output value in generation order, *I* is the input value, *α* is the smoothing factor between *0* and *1*, and *o[v-1]* is the previous output value. An example of such an algorithm 29 integrated is presented below.

Algorithm 29. Efficient Publishing integrated code.

```
# define libraries
#define variables & ports
#define ssid, password, & host to connect
#setup() function for data exchange & monitoring
#loop() function for programming of nodes
  # if((valueA ± 5) ≥ valueB) && ((valueA ± 5) ≤ valueB)
   {
     # publish values to Broker
     # database can migrate data published
```

```
        # apps send database table to a cloud server for
            further analysis
    } else { repeat for the next value }
```

In Figure 51, the TCP-based IoT protocols (Mingqiang Zhu et al., 2017; Rakesh Kumar Lenka et al., 2019) and the UDP-based IoT protocols have noticeable differences in terms of bandwidth and packet loss. Due to the fact that no re-transmission of packets was done, CoAP did not consume any more bandwidth (Annie Gilda Roselin et al., 2019). Also, increased network packet loss was not detected. MQTT increased the bandwidth consumption and the network packet loss, because these are TCP-based protocols and re-transmissions were used to guarantee the packet delivery.

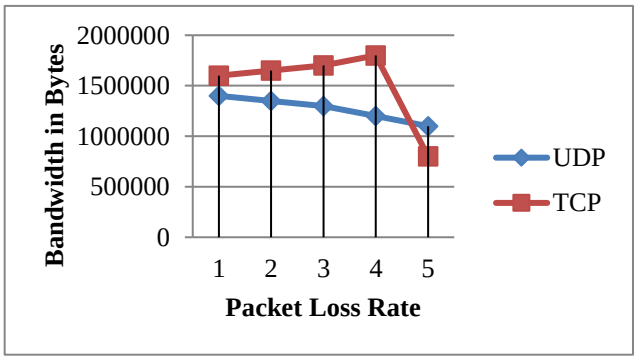


Figure 51. Bandwidth and Packet Loss Rate between TCP and UDP based communication IoT protocols.

On the other hand, frameworks make IoT-networks simpler. The complex interoperability issues such as the interface interoperation, the exposal of data and the functions used can be concealed by the abstraction built for the network devices. To make this happen, an IoT-application has been developed with the Node.js that uses framework APIs. The framework supplies developers with built-in authorization and authentication system which will block the access to unauthorized users and thus, enhances the security of the resources. The framework secures the resources against the most dangerous threats (i.e. SQL injection, cross-site scripting, etc.).

The framework also provides simplicity through an efficient route to enable the authorization logic and to control the access to the data. This PHP framework has also a mailing and notification system across many channels. It is also integrated with cached memory which is used to enhance the performance of the system. This memory is a fast static RAM which boosts the performance of the application in the back-end. Error and exception handling is also provided by the framework in order to help developers solve any issue. It also comes up with built-in functionalities for testing the application.

In this study, the aim is to present an IoT-architecture for a "Smart" environment. The proposed system consists of the layer where the network was built, the middle layer that is responsible for the forwarding of the produced, collected, and selected data and the third layer or the application layer that is responsible for the data abstraction, presentation, and analytics.

The results show that a system requires specific protocols, mechanisms, and algorithms to work efficiently and meet the expected needs. The transmission of the data must follow the appropriate steps in order to increase the bandwidth. Emerging intelligent application technologies and frameworks integrate and use efficiently these IoT protocols. This simplifies the whole process and communication with many IoT and

network protocols and thus, computing complexity and efficient memory management can be maintained by the users' mobile devices.

11.5 Proposition 5

The following architecture has been proposed regarding the work: ***"IoT-based Health and Emotion Care System"*** that has been published in the proceeding of the Elsevier's ICT Express Journal (2022).

In a smart healthcare room, which may be part of a hospital or part of a patient's house, was created a local sensor network. Through this network the doctor can easily connect with patients to a secure and detached network in which they can communicate about and during the healthcare.

More specific, the main purpose of this research is to offer an optimum healthcare environment by using multiple new technologies and techniques. This could be done by establishing a direct network with health and environmental devices. These devices have the ability to communicate over this network (Chatterjee and Armentano, 2015; Luca Catarinucci et al., 2015; Udit Satija et al., 2017; Sean Pham et al., 2020).

The network hosts sensor nodes that produce values over time. These values depending on their quantity can be called "Big Data" (BD). To transmit data generated by the sensors and the images taken by the camera, the "Extensible Messaging and Presence Protocol" (XMPP) seems to be one of the best solutions. The specific protocol is an open standard. It is based on the efficient publish/subscribe model which provides safe and efficient communications. The XMPP also interacts efficiently with the cloud and storage systems and meets all the needs.

The sensors are low-power devices that are connected to a "Broker" in patient's smart device. The Broker is software that holds these values produced over time by the sensor devices under a specific topic. For example, the heart rate values are under the topic "HR". Each value has a weight in order to be recognized among the other HR values. These values will be displayed on smartphone's screen, but not managed or analyzed by the patient in order to keep his/her emotions in a normal level and not in a level that will transform the values.

For example, the temperature of the patient is 36.6 degrees and the patient only sees this number. The sensors used in the proposed network are the heartbeat sensor, the blood volume sensor, the skin conductance sensor, the temperature and the body temperature sensors, the humidity sensor, and a camera device that records eyes and mouth gestures and grimaces. Respectively to the sensor devices there are the topics "HR", "BV", "SC", "Temp", "Humm", "BTemp", and "CD". Then, the Broker holds the values under the specific topics and publishes these weighted values.

All devices are connected to a microcontroller via Wi-Fi or Bluetooth Low Energy (BLE). The microcontroller is then responsible to connect with the Broker and transmit the values through a Bluetooth 5 module or Wi-Fi module to the smart device. The following algorithm (Algorithm 30) presents the programming of the nodes. The "v" in this algorithm means a value specified for each sensor in order to make the comparison and send less data to the broker device.

Algorithm 30. Programming the sensor nodes.

```
#define libraries
#define variables & ports
#define ssid, password, & host to connect
#setup() function  for data exchange
#loop() function for programming of nodes
    # add the produced value in cache memory
   # compare with previous value
   # if((valueA ± v) ≥ valueB) && ((valueA ± v) ≤ valueB){
       # publish value to Broker
       #database and apps can migrate data published
     }
   # else{
       # delete value from cache memory
       # repeat for the next value
     }
```

The application which runs on patient's device was developed in JavaScript with the use of a PHP Framework. The framework itself provides authentication for each patient and privacy. So, after the Broker publishes the topics the application subscribes to these topics and gets the values displayed. The values are immediately stored on a local database under the specified topics. This kind of network offers confined access to the Internet by patients and also provides efficient security for sensitive data interchanged during the patient's care. In the following figure 52, the proposed node communication flowchart for the publish/subscribe protocols has been presented.

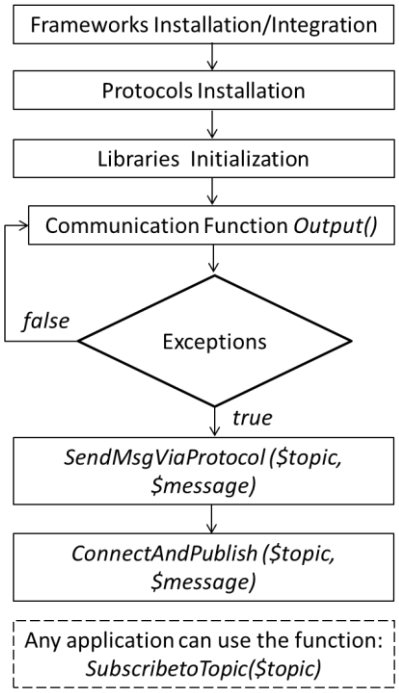


Figure 52. Proposed node communication flowchart for the publish/subscribe protocols.

In the following figure 53, the proposed system architecture can be observed. The system consists of wearable sensors which monitor the patient's health condition and a "Camera Device" (CD). The data are first analyzed locally and then compressed and moved to a cloud server for better analysis. In the local network there is also a WSN which monitors the environmental conditions in the smart room and makes them perfect for the patient's living.

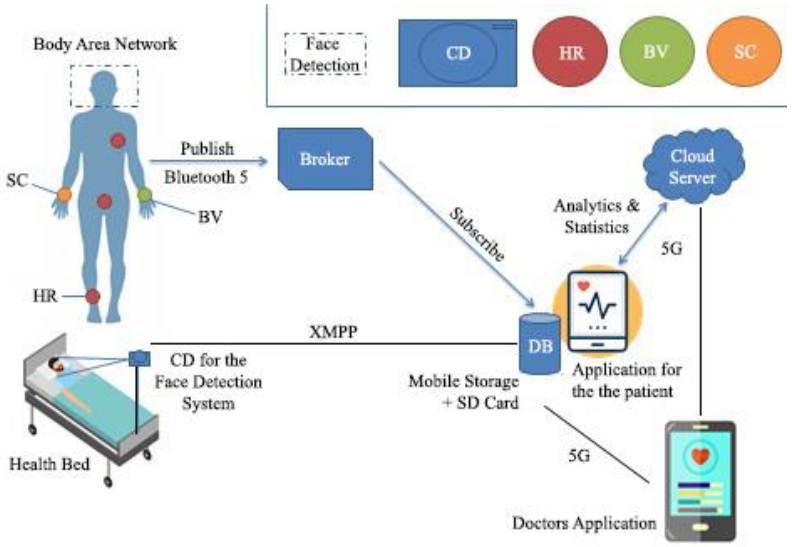


Figure 53. Proposed Network Architecture.

In this research work, the prediction of emotions was taken also into consideration. Since, sensors were used to monitor "Heart Rate" (HR), "Blood Volume" (BV), "Skin Conductance" (SC), and "Body Temperature" (BT) the design and development of an "Emotional Intelligent System" had become a challenge. This intelligent automatic system will be part of the patient's application. While registering, the patient was asked to answer some questions and fill up some fields with personal data such as the full name, the age, the gender, the weight and height, and the fitness levels. Some questions asked to answer are if there is anxiety or irritability, if there is general fear, if there is upset or panic, and how the patient feels in general. Then, the monitoring system can be attached to the patient (Tivatansakul and Ohkura, 2015; Atefeh Goshvarpour et al., 2017; M.-P. Hosseini et al., 2017).

In order to extract knowledge from the signals, two conditions have been taken into consideration, the metrics arousal and valance from the IoT sensors and a machine learning scenario that is based on a "Convolutional Neural Network" (CNN) (Al-Hamadi and Chen, 2017).

About the first condition it can be observed that decreased arousal and increased valence shows that the person rests. Increased arousal and increased valence show that the patient has positive emotions. Decreased arousal and decreased valence means the patient has negative emotions. Increased arousal and decreased valence mean the patient is afraid of something. These four states can describe the feelings of the patient. But there are also some more aspects which play significant role in emotion recognition. (G. Ding et al., 2016; X. Yang et al., 2015)

About the emotional condition, the idea was to use filters so that, knowledge can be extracted from the images which have been taken during the healthcare. Due to that, there is a need to train an algorithm in order to recognize different emotions of a human. To train the efficient algorithm, the TensorFlow framework was used. TensorFlow is an open-source platform for training machine learning algorithms and models. Using this framework and setting multipliers to filter images made possible to group and fit images with same sequences in order to extract features and recognize face/lip-morphisms. (Kalliopi Kyriakou et al., 2019 - Z. Lin et al., 2016)

For the implementation of the emotional condition, the CNN has to make a comparison of the sequences of the images. A CNN is an artificial neural network which organizes these images. Since there are many deformations between images of the same emotion for each person, what we need is to classify all possible and different morphisms into a single unit. To better understand this mechanism the following figure 54 explains in detail how the algorithm was trained for a restful emotion of a person or just a normal lips-morphism.

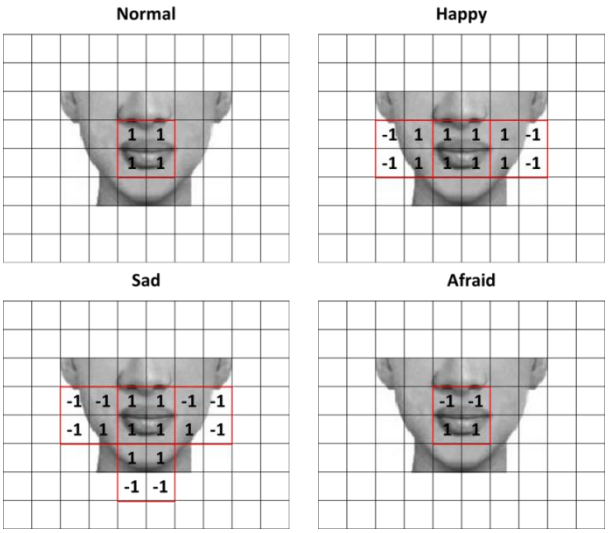


Figure 54. Group of features that match in each image.

Numbers for each pixel of the image were used because computers read numbers in order to understand an image. Number 1 is for the pixels in grey-scale that represent the lips morphisms and number -1 is for the pixels that should not be taken into consideration. Then using normal techniques, the images are compared and pixels with number 1 were grouped.

Moreover, the CNN compares the pixels which are the features that need to be matched in order to recognize the different lips-morphisms for a single emotion. Different groups of features play the role of filters used to understand each emotion. Finally, when the two conditions are compared the emotions can be predicted more accurately.

Let's first train an algorithm for the emotion of happiness. The first step is to check if the parts of the first image are matching the parts of the second image. Since they match, one part is picked up and put on the second image. If these parts match

each other, then, the classification was done perfectly. Moreover, the parts that are marked were moved in all possible positions in the image in order to multiply each pixel of the two images by the corresponding part. After the multiplication what should be done is to add these values and then divide with the total number of the pixels. The result should then be put into the correct cell of the matrix. The same was done for all the parts of the first image. Finally, the output was another matrix which was for one particular pixel. The same should be done for all three parts and the result was three matrices.

Also, all the negative values were replaced with zeros because if they were summarized the result would be zero and that must be avoided. This was done with the use of the following equation 1:

$$\mathbf{G(y) = 0} \text{ for } \mathbf{y<0} \text{ and } \mathbf{g(y) = y} \text{ for } \mathbf{y>=0} \qquad (1)$$

In the final stage the classification was done in which the size was reduced more and the matrix became a single list of elements. From the single list, the elements that were high in exact positions of the list will be for the emotion of happiness. The same was done for the other three emotions.

A "Smart Healthcare-Room" has been installed in a local WSN, in which several functions work. All technologies that have been used offer a novel, efficient, safer and high-speed wireless network in the smart room which consists of sensors and actuators. Some of the network's advantages that are offered are the limited access to the Internet by the patients and as an extension of it offers better protection of the sensitive data that are interchanged. An application has also been developed with the use of various frameworks in order to gain interoperability, authentication of the patient and simplicity.

Moreover, emotions were predicted through the data analysis and through efficient algorithms. Due to these algorithms the healthcare and emotion care system can work together by sharing the same resources. Last but not least, the system integration was advantageous in terms of energy efficiency from other systems proposed. Finally, for further analysis of the data and more storage the mobile cloud computing technology is on the table.

11.6 Proposition 6

The following algorithm has been proposed regarding the work: ***"Efficient Algorithm for Texture Recognition using Haptics over Internet of Things".***

The purpose of this project has been to be able to feel/understand different types of objects, shapes, and textures through a haptic device. Initially, the goal was to write and compile code from scratch to display images on the screen and interact with them through the haptic device. The code that does this job can be observed in the following algorithm 31:

Algorithm 31. Display images on the screen and interact with them through the haptic device.

```
<Scene>
  <Shape>
    <Appearance>
      <Material/>
        <ImageTexture url="Scheme1Plageras.tif" DEF="IMT"
repeatS="false" repeatT="false"/>
        <ImageTexture containerField="depthMap"
url="Scheme1Plageras.tif" repeatS="false" repeatT="false"/>
    </Appearance>
      <Box DEF="FLOOR" size="0.95 0.49 0" />
  </Shape>
</Scene>
```

One is used as the material, ie the material and the other is used as the bump map, ie the color depth (Image Depth Map). Since the images have been displayed, the next step has been to interact with these images. By the combination of color depth, stiffness, damping, static friction, and dynamic friction methods someone can understand the different textures in the images. Such an image can be observed in figure 55 below. The final code can be observed in proposed algorithm 32 below:

Algorithm 32. Final code for texture recognition on images through haptics devices.

```
<?xml version="1.0" encoding="utf-8"?>
<X3D profile='H3DAPI' version='2.0'>
  <head>
    <meta name='title' content='depthMappedSphere.x3d'/>
    <meta name='description' content='An example of how a surface specified
through the DepthMapSurface node can feel. The example only works for
GodObjectRenderer and RuspiniRenderer.'/>
    <meta name='author' content='SenseGraphics AB, 2008-2014'/>
  </head>
  <Scene>
    <Shape>
      <Appearance>
        <Material />

        <ImageTexture url="Scheme1Plageras.tif" DEF="IMT" repeatS="false"
repeatT="false"/>

        <DepthMapSurface stiffness="0.3"
          maxDepth="0.007"
          staticFriction="0.4"
          dynamicFriction="0.2"
          whiteIsOut="false" >

          <ImageTexture containerField="depthMap" url="Scheme1Plageras.tif"
repeatS="false" repeatT="false"/>
```

```
            </DepthMapSurface>
          </Appearance>

          <Box DEF="FLOOR" size="0.95 0.49 0" />
…
        </Shape>
    </Scene>
</X3D>
```

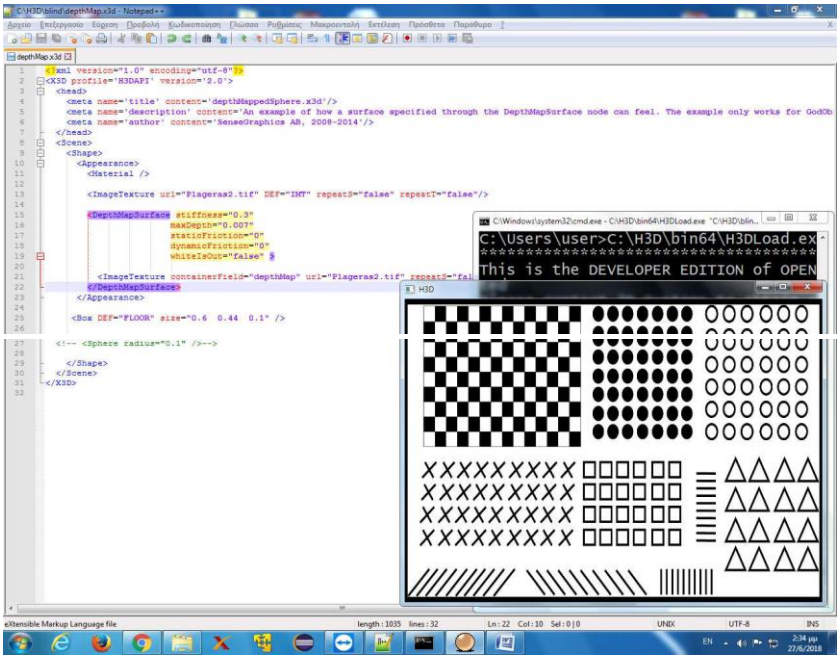


Figure 55. Algorithm and image with different textures.

Chapter 12

Testing, Evaluation, and Experimental Results

The purpose of this dissertation is to combine different technologies, protocols, algorithms, and tasks in order to provide efficient real-time communication that is characterized by low latency, low overhead, security, and low energy consumption. The following propositions 7 and 8 have been implemented and tested as analyzed below.

12.1 Proposition 7

The following architecture has been proposed regarding the work: ***"Digital Twins and Multi-Access Edge Computing for IIoT"*** that will be published in the proceedings of the Virtual Reality and Intelligent Hardware journal and in the Special Issue on Digital Twins (Under Review).

In the first layer (physical), where data generation takes place, the IIoT devices have been initialized and connected to the infrastructure. This is the layer where the data can be managed before, after, and during their generation. Various techniques and algorithms have been put onto the table such as waveform techniques, OFDM (Orthogonal Frequency Division Multiplexing), FBMC (Filtered multi-tone mode of filter bank MultiCarrier), UFMC (Universal Filtered MultiCarrier), GFDM (Generalized Frequency Division Multiplexing), and load balancing algorithms.

In the following table 10, the most common load balancing algorithms have been listed such as the "Round Robin" (RR), the "Weighted Round Robin" (WRR), the "Least Connections" (LC), the "Weighted Least Connections" (WLC), and the "Random".

Table 10. Comparative analysis of load balancing algorithms.

	RR	**WRR**	**LC**	**WLC**	**Random**
Servers with identical specifications	✓	-	✓	-	✓
Supporting critical apps	-	✓	-	✓	-
Overloaded server	✓	✓ / - If connected for longer period than expected	-	-	✓ / - If nodes have different specs

Many researchers have been studying task offloading solutions for the load balancing and distribution of tasks between the edge servers. Akhiruh et al. claims that because of the distance between the local system and the cloud, propagation delay (distance divided by the propagation speed) and fail of synchronization issues due to the increased packet delay deviation (jitter) have been increased between the local

devices and the cloud server (CS). The entire task offloading on the CS can cause further expansion of the completion time of the task. So, a solution to this problem is to make the task offloading on the edge servers (ESs). This will reduce the overhead and improve the traffic congestion and the time needed to respond. (Pydi and Iyer, 2020; Syed Husain et al., 2018; Akhirul Islam et al., 2021; Liu and Liao, 2020; Zichao Zhao et al., 2020; Jun-Jie Yu et al., 2020; C. K. M. Lee et al., 2020)

The purpose of the offloading of tasks to MEC servers is the reduction of the runtime of tasks and the energy consumed by the devices. MEC Servers have not the same capabilities as CS and because of this the utilization of ESs is sensitive. Control-based offloading of tasks provide real-time decision making. (Yuyi Mao et al., 2017)

Therefore, the following hybrid algorithm 33 has been proposed for the load balancing when payload is generated by the devices needs to be transmitted to the edge clusters.

Algorithm 33. Hybrid load balancing algorithm for edge orchestration.

```
S1= Situation1 (non-critical data)
S2= Situation2 (critical data)
v_g = value generated by a device
LB = Load Balancer
EB = Edge Broker
ES = Edge Server
EC1 = Edge Cluster1 of ESs with weights
EC2 = Edge Cluster2 of ESs with weights
CS = Cloud Server
LC = Least Connections algorithm
WLC = Weighted Least Connections algorithm
Initialize LB {
    assign device priorities
    assign weights to ECs and ESs
    assign calculators for connections in ESs
}
Loop() {
   check device priority {device with higher priority first}
   for each v_g do
      check the size && type
      if v_g = S1 then
         publish v_g to the EB
         use LC algorithm to assign request to EC1
         check number of current connections
         ES with preferred capabilities in EC1 subscribes to get v_g
      else if v_g = S2 then
         publish v_g to the EB
         use WLC algorithm to assign request to EC2
         check capacity weights
         select ESs
         check number of current connections in each ES
         ES with least connections in EC2 subscribes to get v_g
      else
```

```
            assign request to CS
            CS subscribes to EB to get v_g for processing
        end if
    end for
}
```

The hybrid algorithm 1 provides load prioritization and payload control in order to meet the desired QoS requirements of the IIoT networks and the best performance of the application running. The Random algorithm would also be a good solution for the critical resources since it provides load distribution, but only when nodes have the same specifications.

In relation to the design of the proposed deterministic multi-hop "Wireless Sensor Network" (WSN), the position of the nodes is fixed, resulting in more simple control and implementation of the system. However, in many cases the location of the nodes is unknown. Therefore, nodes must operate in a dynamic and distributed manner, which provides greater flexibility and scalability, but requires more complex algorithms for the control of the nodes.

The proposed network can be characterized as an aggregating network since the nodes are of big volume in an industry. Each of the nodes is near other nodes and this can cause data redundancy. With the right collection and transmission methods this could be avoided. The results will be less network congestion and less energy, but increased computing performance and memory. In figure 56, the proposed communication model of the multi-access edge-cloud framework can be observed.

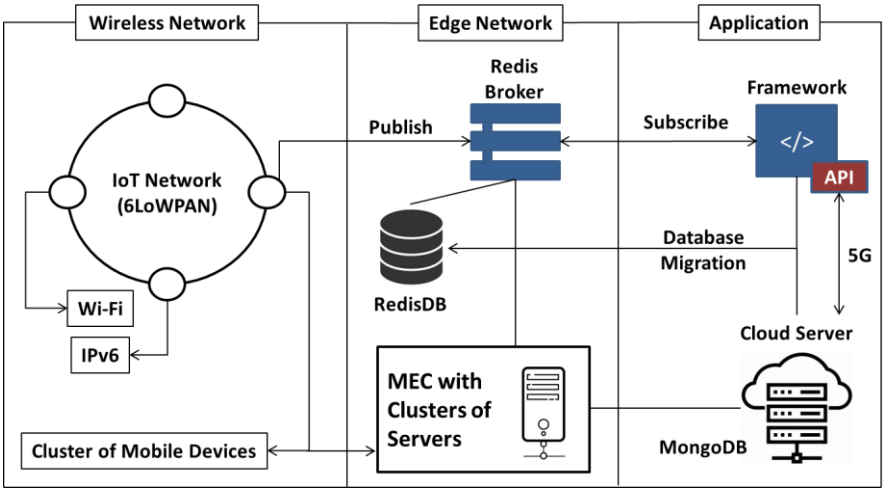


Figure 56. Proposed IIoT communication model.

The "Contiki Operating System" (OS) has been also used with its' useful applications for network design and testing. A great number of emulations in the "Cooja Emulator" have been run in order to measure in a single cluster the network performance, the energy consumption, the packet loss, the latency, the routing metrics, the protocols performance, and some more that will be discussed later in this section.

In figure 57, a network cluster of mobile devices that has been implemented and run for thirty minutes with Cooja can be observed.

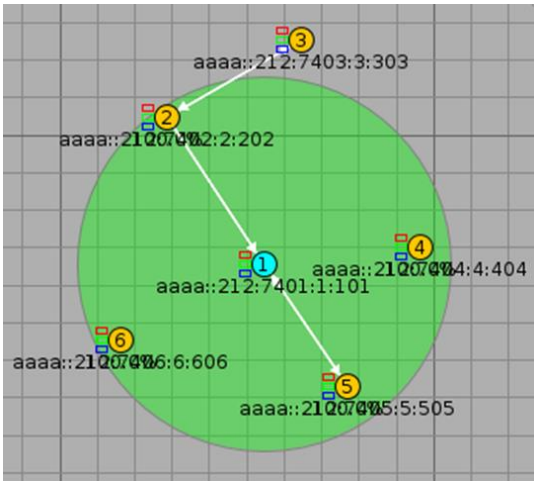


Figure 57. Device cluster simulation for 30 minutes.

The specifications of the specific cluster in the network have been presented in table 11 below.

Table 11. Specifications of the specific cluster	
Operating System/Simulator	Contiki OS 3.0 / Cooja Emulator
Radio Medium	Unit Disk Graph Medium (UDGM): Distance Loss
Operating Frequency	2.9 GHz
Data Rate	250 kbps
Protocols	6LoWPAN, IEEE 802.15.4, RPL, CoAP
# of nodes	6
Tx/Rx	50m x 50m
Runtime	1800sec
Packet Size	127 bytes
PHY and MAC Protocol	IEEE 802.15.4 and CSMA/CA
Type of Mote	Sky Mote

In figure 58, the battery life can be observed. It is one of the most important aspects that must be considered and tested during IoT development. The dissatisfaction of users, the decreased battery life, and the increased cost are some of the results of avoiding measuring the energy consumption of a system, platform or application. For the energy consumption estimation of an application, the measurements could be held with specific software, but when comes to the IoT platform, then the complexity is at high levels.

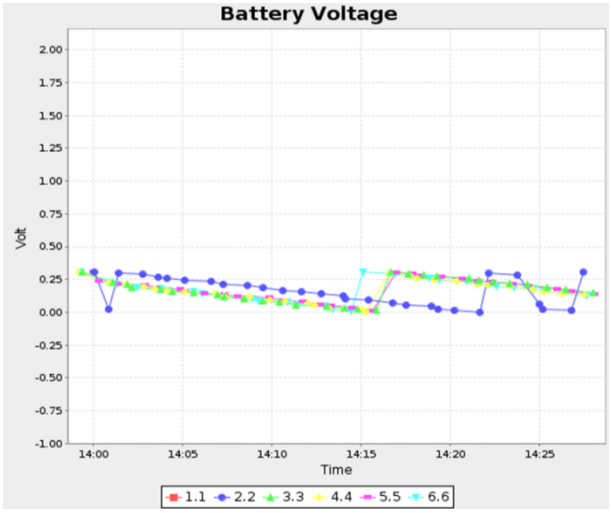


Figure 58. Battery Voltage for 30 minutes of continuous communication.

In figure 59, the historical power consumption in mW per second has been shown, in figures 60 and 61, the instantaneous and the average power consumption can be observed respectively. Both figures show the consumed energy by the LPM (Low Power Mode), the CPU, the radio listen, and the radio transmit. The energy consumption of each node has been calculated based on following equation 1:

$$P_{CON} = (EV * Curr * V) / (RTsec * Runtime) \quad (1)$$

where P_{CON} is the power consumption, EV is the energest value, Curr is the current, V for voltage), RTsec the "timer" in seconds, and the Runtime the time the simulation runs.

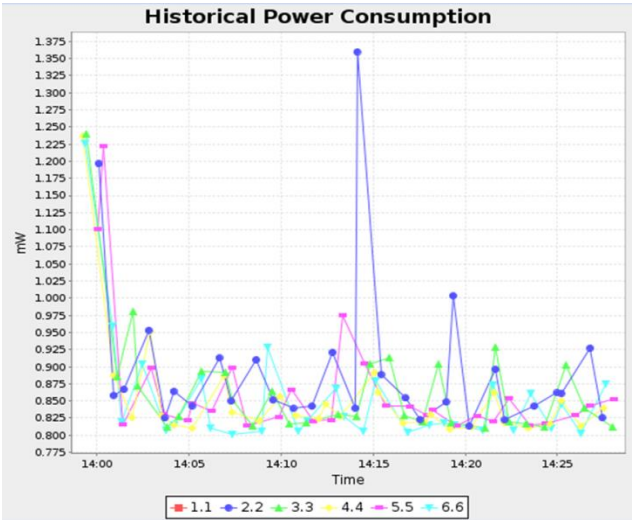


Figure 59. Historical power consumption in mW per second.

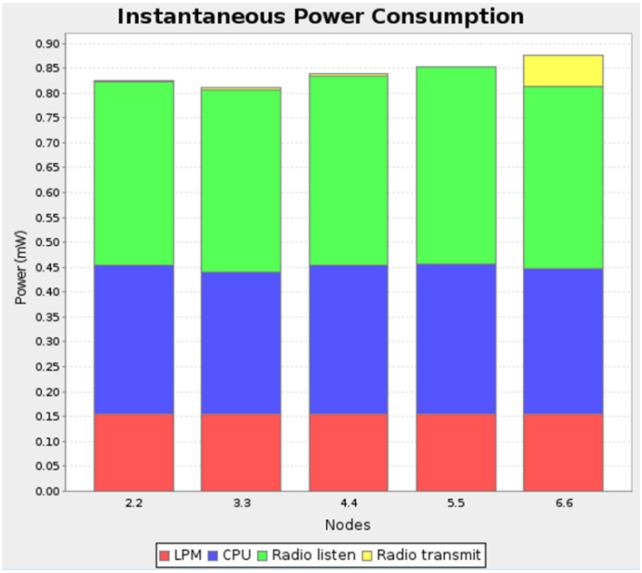


Figure 60. Instantaneous Power Consumption.

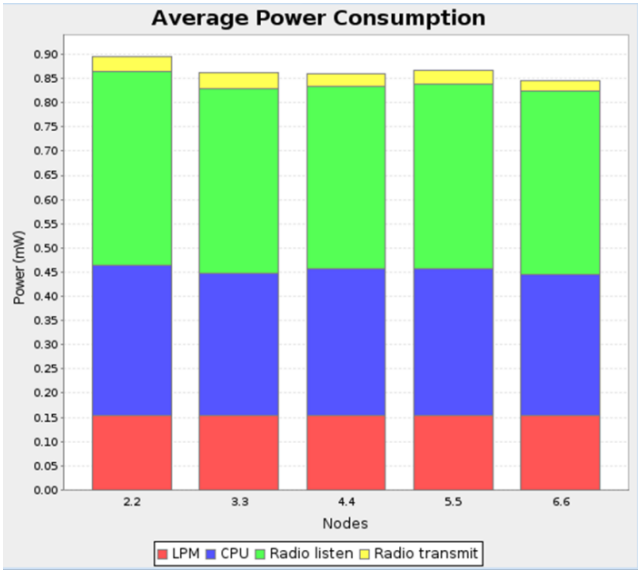


Figure 61. Average Power Consumption of each node.

Moreover, a "Low power and Lossy Network" (LLN) usually uses battery constrained motes. Thereafter, in order to measure the energy consumption of the network the time the mote is on can be divided by the time interval. This will give the "Average radio duty cycle" of the network which has been presented in figure 62 and can be described with the following equation 2:

$$ARDC = T_{on} / T_{int} \qquad (2)$$

where T_{on} is the time the mote is on and T_{int} the time interval.

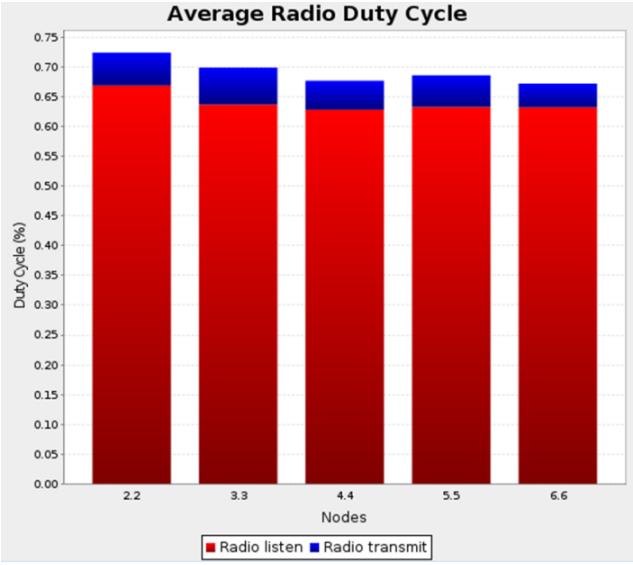


Figure 62. Average radio duty cycle.

Figures 63 and 64 present the estimated time of transmissions (ETX to next hop) and the received packets per time respectively.

To estimate the reliability of the network the following equation 3 has been used, which estimates the "Packet Delivery Ratio" (PDR):

$$PDR = Packets\ Received / Packets\ Transmitted \qquad (3)$$

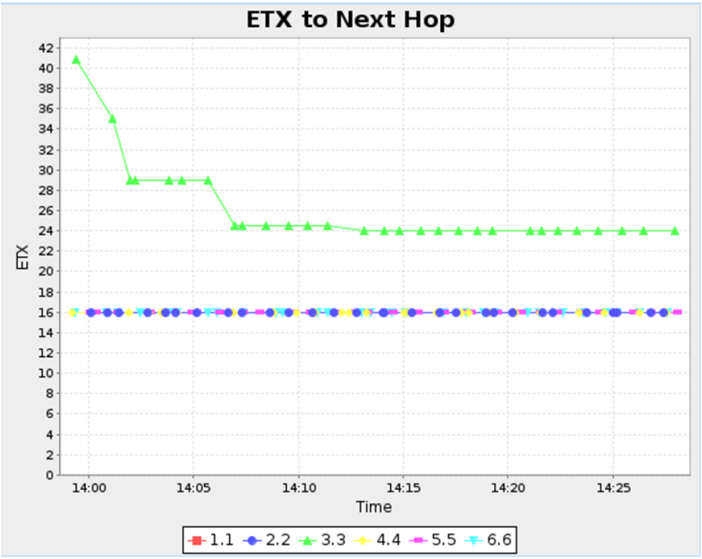


Figure 63. Estimated number of transmissions (ETX to next hop).

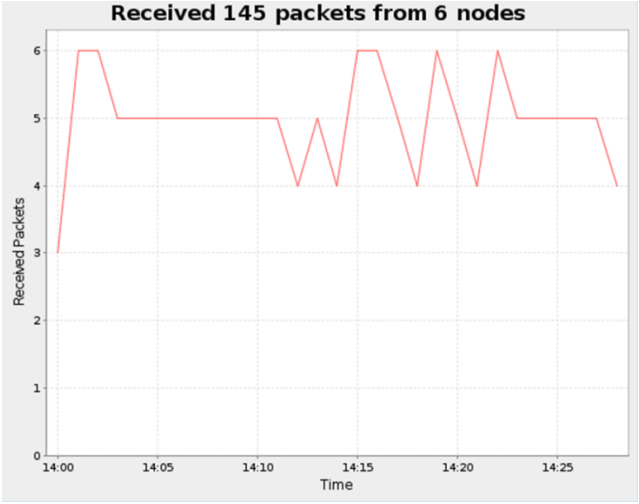


Figure 64. Received packets per time.

In figure 65 the routing metric per time has been provided.

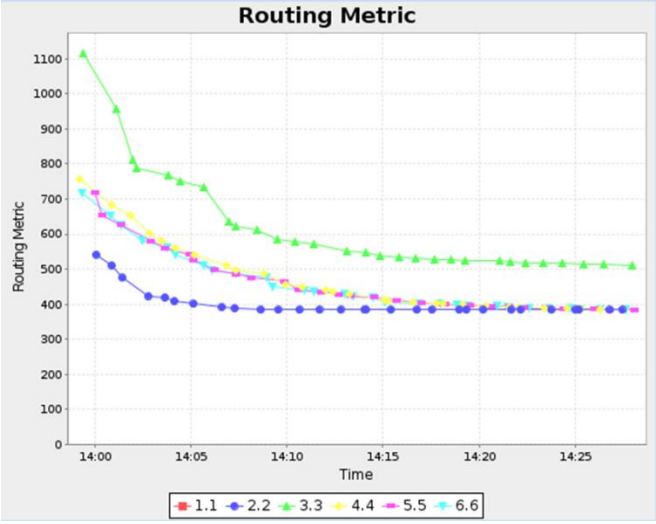


Figure 65. Routing metric per time.

The middle layer of the proposed framework is a combination of two non-relational databases (NoSQL) that play a key role in the whole system since they provide flexibility and scalability in real-time applications. Such databases are the MongoDB and Redis.

Redis acts as a broker that delivers messages and thus, it has been used in the edge-fog layer for real time communications and if needed it can also serve in the cloud. In addition, it has been used as local database and cache storage. It serves the processing of the data even on heavy situations in a few milliseconds. The MongoDB has been studied and configured also inside the framework as a database for specific volume of data and in order to efficiently handle the big amounts of data produced by the IoT devices. It also provides cloud services.

Figure 66 demonstrates the system model and flow. Specifically, the devices have been divided into clusters depending on the feasibility of each device, the critical and non-critical resources and thus priority of devices. The flow of the data generated by these clusters and the different protocols used can also be observed. Furthermore, the proposed middleware has been shown next, which consists of clusters of edge servers (ESs) - two clusters in count - that can manage the loads with the use of suitable algorithms depending on each occasion which provide real-time results (analytics) to end-mobile-users. Also, this layer consists of broker devices, which can handle efficiently the communication and publication of the data, and the conjunction of the two aforementioned databases. Then, a cloud server (CS) can access the data by subscribing to the ESs or by migrating data from the database system. Last but not least, the CS responds with the results from the 'deep' analysis of the data.

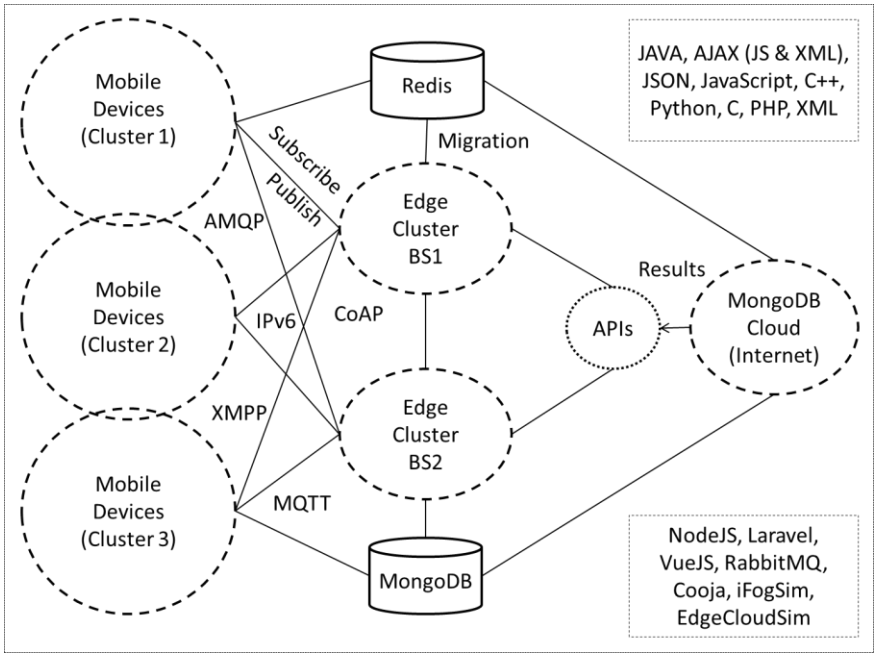


Figure 66. Proposed IIoT Multi-Access Edge Framework architecture.

The API (Application Programming Interface) has been developed with the Laravel Open-Source PHP-framework. This framework provides the DOM (Document Object Model) of the API. In simple words, it contains a structure for efficient application development and it is based on the MVC (Model-View-Controller) architecture. (Liu and Liao, 2020; Zichao Zhao et al., 2020)

The application which runs on the mobile device has been developed by combining two frameworks: the Laravel and the VueJS. These frameworks provide authentication for the user and therefore for the device.

To begin with the evaluation of the proposed scenario, the open-source "EdgeCloudSim" simulator has been configured in order to simulate the MEC scenario. There have been carried out multi-tier with edge orchestrator (EO) scenarios, which use many servers (edge and cloud). This simulator uses five memory management

algorithms that have also been tested and the results have been listed in the following table V.

These are namely Random_Fit, Worst_Fit, Best_Fit, First_Fit, and Next_Fit. Random_Fit allocates a random block of memory from a group of chosen blocks that were tracked. This algorithm has a complex implementation. Worst_Fit allocates to the biggest partition one process, but if another big one arrives it could not be allocated. Best_Fit allocates to the smallest partition the process arrived. First_Fit introduces the internal and external fragmentation issues. The first is caused by allocation of memory slices at the starting point of the memory. The second one is caused by the slicing of partitions while looking for an empty one and thus a big process which arrives is dropped. Next_Fit which is an extension of First_Fit, but it starts the next search from the last point.

In the next two figures 67 and 68, the number of tasks completed in 4 different application domains and the number of completed and failed tasks on edge and cloud have been presented respectively.

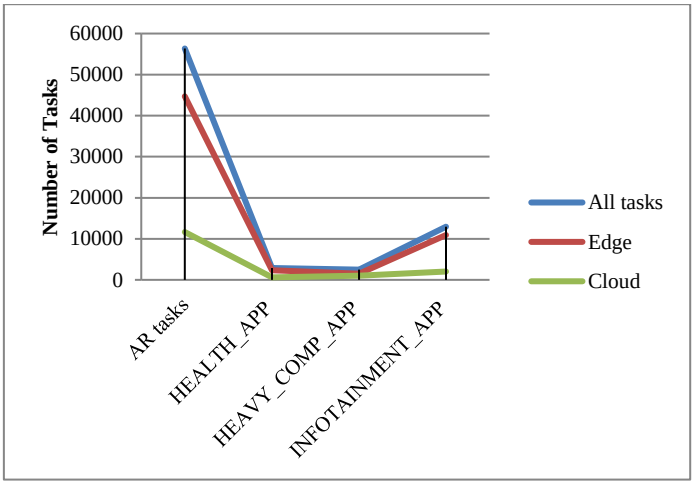


Figure 67. Number of tasks in different application domains.

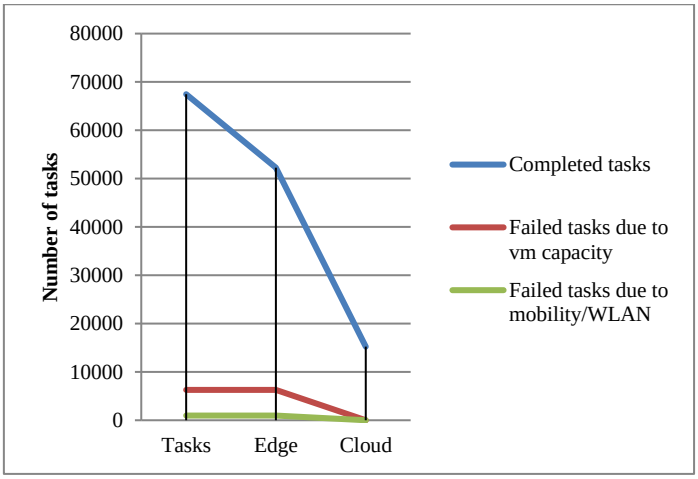


Figure 68. Number of completed and failed tasks in edge and cloud.

In this section, there have been provided the results from the tests carried out to evaluate the proposed framework. To begin with a comparative analysis among various implementations and the proposed one, table 12 below has been demonstrated.

Table 12. Comparative analysis of the proposed framework among others

	(Hsiao and Lee, 2021)	(Hui Zhou et al., 2021)	(Aidan Fuller et al., 2020)	(Akhirul Islam et al., 2021)	Proposed
MEC	-	✓	✓	-	✓
FC	-	-	✓	-	✓
Cloud assisted	✓	✓	✓	✓	✓
IIoT	✓	✓	✓	-	✓
Network	5G	5G	5G	6G	4G - 5G
ML	✓	-	-	-	-
DL	✓	-	-	-	-
Performance	High	-	High	High	High
Security	✓	✓	✓	✓	✓
Energy Efficiency	✓	-	-	High	High
Latency	-	Low	Low	Low	Low
Data Rate	-	High	High	High	High
Overhead	-	-	-	-	Low
Transmission Speed	-	-	High 1 sec in fog and 16 sec in edge	High (3-5sec)	High
Interoperability	✓	✓	✓	✓	✓
Flexibility	✓	✓	✓	✓	✓
Adaptability	✓		✓	-	✓
Scalability	✓	✓	-	-	✓
Reliability	High	-	-	✓	High
Broker	-	-	✓	-	✓
Mobility	-	✓	✓	✓	✓
Caching	-	-	-	✓	✓
Algorithms for caching	-	-	-	LFRU (LRU + LFU)	Hybrid (WRR & WLC)
Task Offloading	-	-	-	-	✓
Load Balance	-	-	-	-	✓
Complexity	Medium	-	-	Low	Low

From table 12, it can be deduced that the proposed framework meets the design requirements. (Jun-Jie Yu et al., 2020)

Specifically, the QoS parameters like the low latency, the bandwidth, the data loss ratio, the jitter, the payload prioritization, and the control of the load have been analyzed. In addition, due to the real-time capabilities the proposed network can handle multiple critical and non-critical applications with no interference. The network devices and ESs have been grouped into clusters. These clusters are capable of handling the big variety of devices and thus, ensure the segmentation of the proposed network. Moreover, reliability has been obtained since the load has been delivered efficiently and in the expected order.

By using the load balancing algorithm there can be observed that the convergence speed and system utilization have been at high levels, the processing time for training has been even lower due to the ES with lower load selection, the competition of notes has been reduced, and the average delay among the users has been also reduced.

Confidentiality and integrity have also been guaranteed by the authentication of each device and user. The proposed network can easily be configured again to integrate new devices if needed.

The complexity of the proposed algorithm is of high importance since a wireless, low power, and lossy network consists of constrained devices in terms of energy consumption. To measure the complexity the capacity, the load, and the energy have been taken into account. In the proposed system the complexity has been kept in low levels.

The novel technology of "Multi-Access Edge Computing" or "Mobile Edge Computing" (MEC) has been studied. MEC offers scalability, reliability, security, and efficient control and storage of the data. The proposed algorithm provides efficient data delivery and task offloading. Moreover, results have shown that processing, security, complexity, control, energy consumption, and reliability have been enhanced. Also, the proposed framework and application provides authentication and integrity to the end-users and to the devices.

12.2 Proposition 8

The following security model has been proposed regarding the work: ***"Secure Edge Communications over the IoT"***.

The security model has been proposed for critical sectors, such as healthcare, transportation, industries, etc., which need efficient solutions to go one step further and improve living and production. The proposed secure communication model can be observed in the following figure 69.

In order to successfully attach the proposed architecture in the power and memory constrained IoT devices several metrics have been considered. Such metrics that must be measured and taken into consideration have been the complexity, the throughput of encryption and decryption, the energy consumption, and the memory needed by the devices. All these have been analyzed in the next section comprehensively in order to provide a better insight for future implementations.

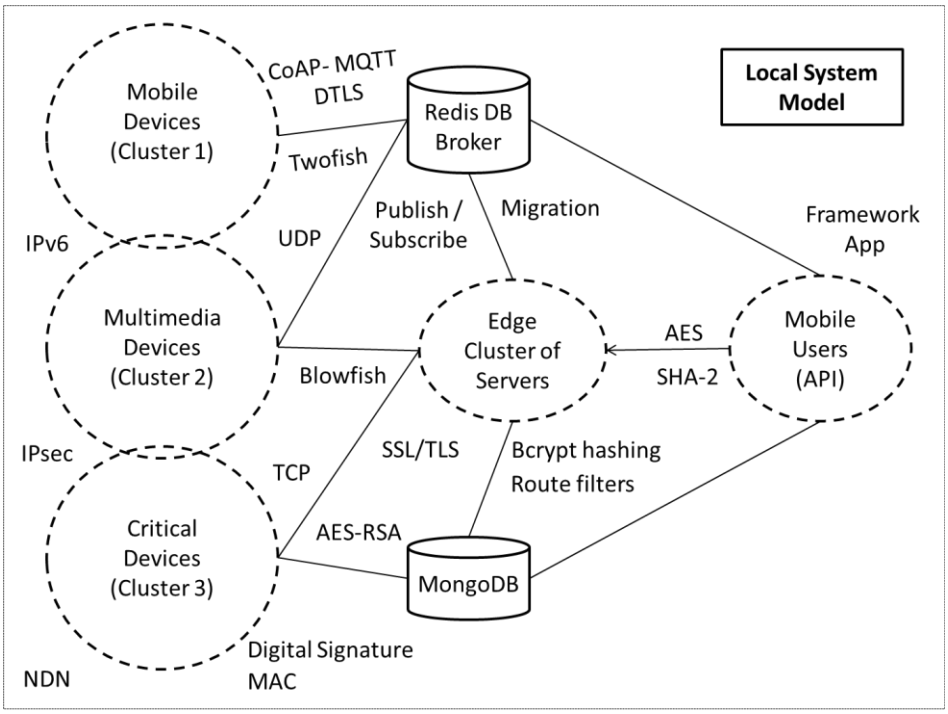


Figure 69. The proposed secure communication model

To begin with the first layer (Physical-Abstraction Layer), many challenges and issues that need a solution have been addressed by various researchers. In this layer, the hardware components must first of all be protected by strict security rules and equipment (such as cameras and sensing devices) in order to ensure their safety from inside and outside the facilities. So, a solution to that problem could be given by AI and machine learning algorithms that will ensure that everybody inside and nearby the facility will be monitored and identified (Lin Shi et al., 2021; Zhihan Lv et al., 2021; Taher M. Ghazal, 2021).

The identification can work in conjunction with a police database table, which will inform with a simple notification message both the facility's security-staff and the nearest police department. Firstly, an image will be captured using surveillance equipment (Depth Cameras) and then this image could be compared with the images stored in a database, in order to measure the similarity through an efficient probabilistic model. Thereafter, a machine learning scenario takes action. This model, while violation cannot be possible on the personal data of pedestrians, will detect specific face features and gestures. The use motion sensors that detect pedestrians' distance from a selected safe point and enables the nearest camera devices when needed. The detection of suspicious motions could be performed with the use of the relevant deep learning algorithms.

The second layer is the middleware, where the edge servers and the databases have been established. In this layer, the networking of the devices has been done by communicating with the first layer. Then, the networking of the users has been done by communicating with the application layer. Each device has been communicating with a specific cluster of servers, where load balancing and task offloading algorithms and

techniques have been performed, depending on the criticalness of each device. In this layer, AI and deep learning algorithms could be used for the sensitive, complex, and important actions.

The databases that could be possibly used in the middle layer are the Redis and the MongoDB. Redis supports “Transport Layer Security” (TLS) and allows access to the topics only by authorized and authenticated users. It also provides a protected mode, in which communicates with queries from the loopback interfaces, and sends an error message to clients connecting from other addresses. Injection is not possible under normal circumstances by using a normal client library. The protocol is binary safe and is using prefixed-length strings.

The third layer is the application-presentation layer, where the application lives and the presentation of the data has been performed. First of all, the mobile users should have rich or sufficient authentication mechanisms, secured accounts, access control mechanisms, strong encryption methods etc. These mechanisms have been provided by the framework that has been used for the development of the MVC (Model-View-Controller) client architecture.

The implementation of all aforementioned security algorithms has been done using the Java and C++ languages, but could be implemented the same way in all languages. In the algorithm 34 shown in figure 48 below, can be observed the two implemented methods for encryption and decryption using the Blowfish security algorithm.

Algorithm 34. Implementation of the Blowfish security algorithm.

```
Secret Key = “******”
Algorithm = “Blowfish”
Mode = “Blowfish/CBC/PKCS5Padding”
IV = “******”

Encryption method {
        Create new Secret Key Specification with method getBytes()
        Create cipher = getInstance(Mode)
        Cipher initialization (Encrypt Mode, Parameter Specification)
        Use doFinal() method at Byte[ ] for cipher
        return encoding values in string
}

Decryption method {
        getDecoder() method to decode value
        Create new Secret Key Specification with method getBytes()
        Create cipher = getInstance(Mode)
        Cipher initialization (Decrypt Mode, Parameter Specification)
        return new string with doFinal()
}
```

In this section has also been provided a performance analysis based on different security aspects. As it has been assumed by many researchers the performance of block ciphers

is related to block and key size. The larger the block size is, the fastest the algorithm is. This is because big amounts of data will be encrypted in only one execution cycle. Likewise, the smaller the block is, more execution cycles will be needed and thus, total execution time will be increased. If the key size is very large, this will have negative consequences (slows down) in the performance of the security algorithm, although it enhances the security.

In the following table 13, a comparative analysis of the most known and used algorithms has been done and presented. The table 13 is based on the comparative analysis section.

Therefore, the outcomes from the table 13 below show that the AES, Blowfish, Twofish, IDEA, and TEA security algorithms are advantageous in terms of security, performance, speed, complexity, flexibility, and efficiency. Thus, it has been considered that each algorithm suites different in each IoT use case. So, a combination of the best suited algorithms will provide better and faster security, flexibility, and efficiency in each IoT layer.

In order to make the selection easier, a comparative analysis of the complexity of the two types of ciphers has been provided. The results, which can be observed in figure 70, show that the block ciphers are the best choice for the constrained IoT devices.

Table 13. Comparative Analysis of Modern Security Algorithms

Reference	Algorithm	Cipher Type	Block Size	Key Length	Round (s)	Speed	Security	Disadvantage	Use cases
(Dr. Sam Rizvi et al., 2011; Hassan and Hoomod, 2021; Mohammed Nazeh Abdul Wahid et al, 2018; Ljubomir M. Vracar et al., 2019)	**AES**	Symmetric – Block Cipher	128, 192, 256 bits	128, 192, 256 bits	10, 12, 14	Very Fast	Excellent – widely used	Vulnerable in Timing Attacks	Wi-Fi, processor, websites, mobile apps, VPN
(Rana M Pir, 2016; Hassan and Hoomod, 2021; Mohammed Nazeh Abdul Wahid et al., 2018)	**RSA**	Asymmetric – Block Cipher	Variable	768, 1024, 2048, 4096 bits and more	1	Slow but more functional	Excellent	Vulnerable in Brute Force Attack, Timing Attack, Mathematical Attack, and Chosen Ciphertext Attack	Number Factorization, used in IoT apps, commonly found in SSL/TLS certifications, email encryption, and crypto-currencies.
(Mohammed Nazeh Abdul Wahid et al., 2018)	**DES**	Symmetric – Stream Cipher	64 bits	56 bits	16	Moderate	Insecure – out of use	Low encryption key length, susceptible to brute-force attacks	Financing, Government, Banks
(Mohammed Nazeh Abdul Wahid et al., 2018)	**3DES**	Symmetric – Block Cipher	64 bits	168 (3*56) bits	48 (3*16)	Slower than DES since it is applied 3 times	Vulnerable –due to be replaced	will be phased out as an IoT encryption method by 2023	Financing, TLS protocol, Microsoft Office, Firefox, and in payment systems
(Nuzhat Khan et al., 2017; Dr.	**Twofish**	Symmetric	128 bits	256 bits	16	Overtakes AES,	More secure but slower	Slow	Network apps and Situations with limited

Sam Rizvi et al., 2011)						Quick and Adaptable			RAM & ROM, password security and generation, and encryption of files
(Nuzhat Khan et al., 2017; Mohammed Nazeh Abdul Wahid et al., 2018)	**Blowfish**	Symmetric – Block Cipher	64 bits	Variable Length (32 to 448 bits)	16	Fast	Excellent	Weak key	Payments & protection of passwords, secure shell, secure telephony, OS, file and disk encryption, backups, encryption libraries and toolkits, and database security
(Hassan and Hoomod, 2021)	**Rijndael (AES)**	Symmetric	128 bits	128, 192, 256 bits		Very fast	Excellent	-	Wi-Fi, processor, websites, mobile apps, VPN
(Nuzhat Khan et al., 2017; Hassan and Hoomod, 2021)	**Serpent (AES)**	Symmetric	128 bits	128, 192, 256 bits	32	Very fast	Excellent	-	Wi-Fi, processor, websites, mobile apps, VPN
(Nuzhat Khan et al., 2017; Hassan and Hoomod, 2021; Kolhe and Raza, 2013)	**ECDH**	Asymmetric		Variable (250 bits)		Slow	Excellent	-	End-to-end encryption and post-compromise security
(Nuzhat Khan et al., 2017; Hassan and Hoomod, 2021; Kolhe and Raza, 2013)	**ECDSA**	Asymmetric		Public key: twice the size of the security level, in bits. Private key: 1024bits		Slow	Excellent	difficulty of implementation, design flaws which reduce security in insufficiently defensive implementations	Bitcoin transactions
(Ljubomir M. Vracar et al., 2019)	**El Gamal**	Asymmetric		768, 1024, 2048, 4096 bits and more		Slow	Depends	not secure under chosen ciphertext attack	Hybrid cryptosystems
-	**SRP**	Asymmetric		Large private key shared		Faster than Diffie-Hellman	More secure than SSH	-	
-	**DSA**	Asymmetric		Signature consists of two 160 bits numbers generated from msg and private key		Slower than RSA in encryption and signing but faster in decryption and verification	Equal in strength to RSA	-	Enables IoT products to comply with government security protocols

(Hassan and Hoomod, 2021)	**IDEA**	Symmetric Block Cipher	64 bits	128 bits	8	Very fast in encryption time	Excellent	Weak keys	Constrained Devices
(Nuzhat Khan et al., 2017) (Mishra and Acharya, 2021; Hassan and Hoomod, 2021; Ljubomir M. Vracar et al., 2019)	**TEA**	Symmetric Block Cipher	64 bits	128 bits	Variable Suggested 64 rounds	Fast	Bad as cryptographic hash function	Suffers from equivalent keys, susceptible to a related key attack	Constrained Devices

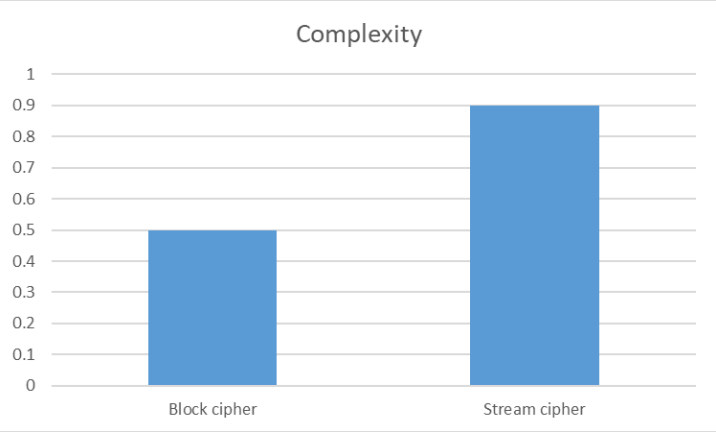


Figure 70. Comparing the complexity of block and stream ciphers.

In figure 71 below, the results from the comparative analysis of AES and RSA security based on the key length have been provided.

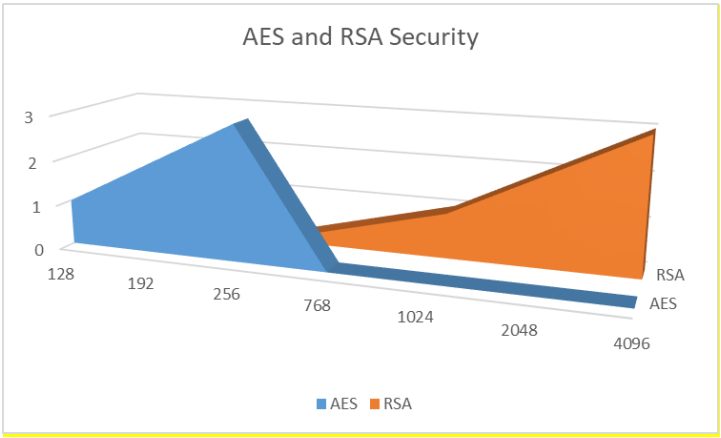


Figure 71. Comparative analysis of AES and RSA security.

In figure 72 below, the results from the comparative analysis of security algorithms based on the equation of encryption throughput below have been provided.

$$Encryption\ Throughput = \frac{Bytes\ of\ PlainText}{Encryption\ Time} \quad (1)$$

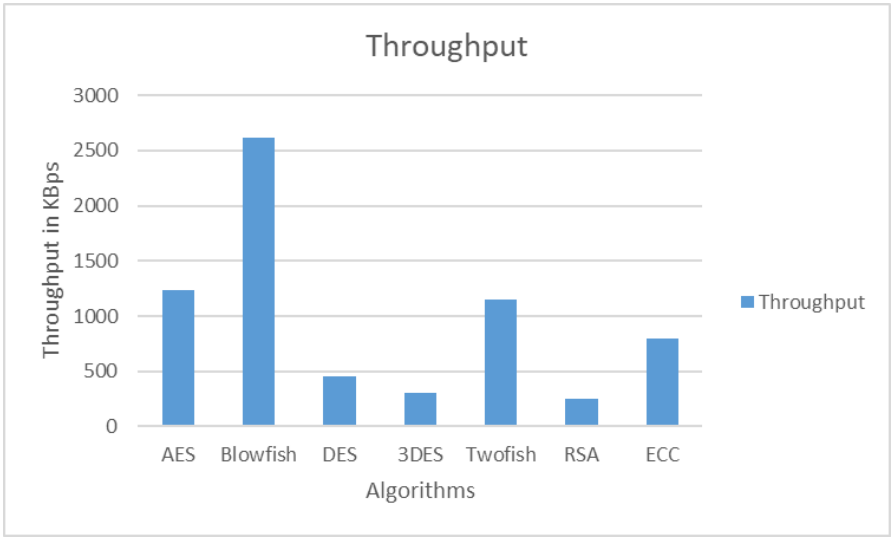


Figure 72. Comparing security algorithms based on throughput.

The energy consumption has been measured using the following equation 2:

*Energy Consumption = Voltage * ElecVol * CCyc * T* (2)

where, ElecVol is the electricity volume, CCyc is the number of clock cycles, and T the period.

The following figure 73 shows the energy consumption measured with the use of the above equation 2 for each of the compared algorithms. (Ljubomir M. Vracar et al., 2019)

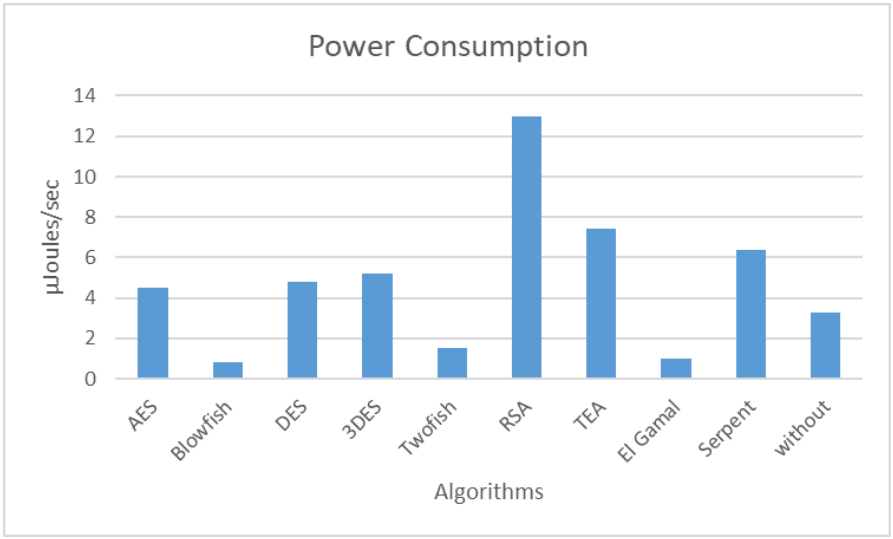


Figure 73. Energy Consumption of Security Algorithms.

An algorithm's strength is based on the size of the key. So, from table III above, the following figure 74 has been constructed.

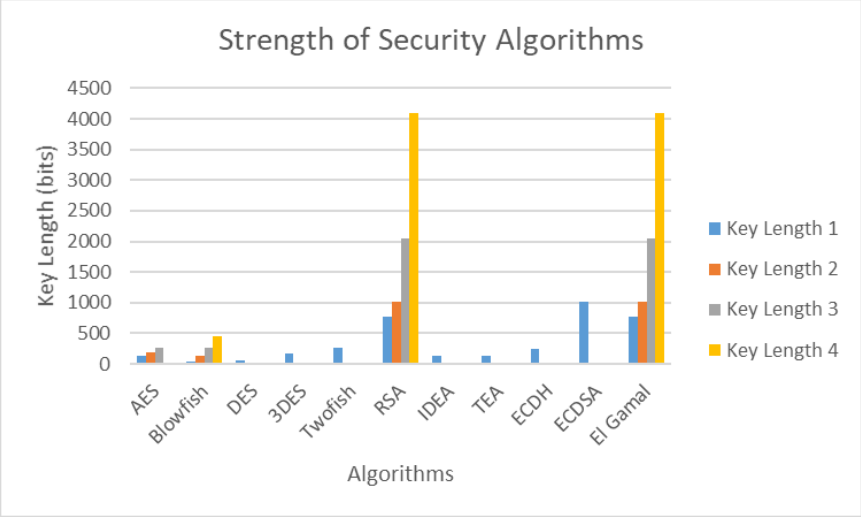


Figure 74. Algorithms' strength based on the key size.

To start with the basic security problems, there have been listed the interception problem, the spoofing problem, the falsification problem, and the repudiation problem. The solution for the interception problem is the encryption of data. The solutions for the spoofing and falsification problems are the "Message Authentication Codes" (M.A.C.) and the "Digital Signature". Finally, the solution for the repudiation problem is again the "Digital Signature". A very commonly used security algorithm is SHA-2 which has been widely used. This algorithm is based on "Hash Functions".

Confidentiality and data integrity have also been guaranteed since each device and user has been authenticated. The hash class provided by the framework for the authentication is based on "Bcrypt hashing" (Password-Hashing function based on Blowfish cipher) and the "Auth::attempt" method. "Route filters" could also be added to give access in a specified route only to authenticated users. The framework also provides CSRF (Cross-Site Request Forgery) protection and gives a solution to the cross-site request forgeries by just using a single method. AES encryption has also been provided by the framework.

Chapter 13

Contribution and Novelty

The findings of this dissertation add to theoretical and practical scientific understanding. From a theoretical standpoint, various frameworks and architectures have been presented that can combine any data transport protocol for real-time communications across the Internet. In the general scientific topic of "Wireless Sensor Networks," these frameworks, topologies, and protocols will adapt to diverse types of sensors (WSNs).

Furthermore, energy consumption has been assessed and taken into account, as it is critical to IoT system efficiency and the capacity to apply more complex security algorithms. So, after extensive investigation and study, the best technique to protect communicated and stored "Big Data" has been proposed in this dissertation (BD).

The proposed IoT communication model has received special attention from the standpoint of applied scientific knowledge. The three layers of this model have been deployed, tested, and evaluated in a variety of projects, using a variety of tools and in a variety of settings. The installation and programming of many IoT devices, surveillance devices, haptic devices, broker devices, and databases has been completed. Finally, application development and systems programming have been thoroughly investigated. To support IoT technology, new frameworks, applications, and algorithms have been integrated too.

This dissertation's general purpose is to integrate new technologies and make them more accessible and available to everyone with an Internet connection from wherever. By integrating new technologies and utilizing sensors, actuators, cameras, and other components and devices, anyone can monitor, manage, analyze, and reap all of the benefits of IoT technology. As a result, everybody can improve his or her quality of life.

This dissertation's major goal is to research and provide relevant algorithms, methods, scenarios, and tools for more efficient BD transmission, management, analysis, energy efficiency, and security. The main purpose of this dissertation was to investigate and research modern technologies, integrated systems, architectures, procedures, protocols, algorithms, and other concepts linked to diverse IoT applications.

Initially, technologies and open issues in general, as well as the interconnection and communication of various sensors, haptic, and other devices, have been investigated. The focus of the inquiry was therefore on the networking of these devices and the transmission of "IoT-BD." Furthermore, in order to increase data security during production, transmission, and storage, security algorithms and methodologies have been researched and compared. Also, the devices' energy efficiency has been taken into account to maximize the energy resources available for proper and efficient operation of these networked devices.

Finally, this dissertation presents novel and original concepts, methods, algorithms, procedures, and technical advances, all of which will improve the quality of life by saving time, energy, and money in an efficient and secured environment.

Chapter 14

Conclusions

To strengthen and promote the "Internet of Things" (IoT) industry, all new technological findings might be included and combined. The revolutionary technology of "Multi-Access Edge Computing" or "Mobile Edge Computing" (MEC), as well as "Digital Twins," is fast gaining traction in the business. MEC serves as a bridge between mobile devices and the cloud, providing scalability, dependability, security, efficient resource control, and storage.

Furthermore, digital twins constitute a communication paradigm that will improve the overall system's latency, overhead, and energy usage. The overall focus of the study is on the most significant difficulties that IoT researchers must address in order to achieve a more effective communication environment in terms of technology integration, efficient energy, data delivery, storage spaces, security, and real-time control and analysis.

First, appropriate algorithms have been configured, installed, and programmed for IoT, surveillance, haptics, and other devices. The databases and the broker devices were then deployed and programmed to function with the IoT devices effectively. Furthermore, a framework has been proposed for reducing traffic and latency by combining the processing of data generated by IoT devices at the network's edge.

In order to determine the optimal decision in each scenario, machine learning methods were also tried and compared. Critical components of the proposed IoT systems were evaluated using emulation/simulation software as well as in real situations with real devices.

The findings revealed that data transport and offloading were more efficient, energy consumption and processing have been improved, and security, complexity, control, and dependability have been also improved.

Chapter 15

Future Work and Future Directions

As future work, it will be managed to integrate more protocols into the proposed framework in order to fill all the gaps of the interoperability problem that IoT faces. Such protocols are the "Modbus", the "WebSocket", the "OPC UA", the "MTConnect", the RPL (Routing Protocol for Low-Power and Lossy Networks), and many more.

Also, as a future research it has been planned to build an emulator (such as EdgeCloudSim and Cooja) in order to gain more accurate results and build even more realistic scenarios.

Moreover, a future work will be to compare all ML algorithms in order to propose novel ways of managing and training data and IoT systems. Similar scenarios to those presented in this dissertation will be realized in the future, not only for hospitals, enterprises, and governments, but also for internal organizations, systems, and networks. Data learning solution can then expand the systems' behaviors in order for them to become stronger and smarter.

Furthermore, mobile cloud computing technology is on the table for future research and greater data analysis and storage space. Finally, data learning technologies and algorithms, as well as artificial intelligence (AI), will be researched and used in the near future.

References

A. Aijaz, M. Dohler, A. H. Aghvami, V. Friderikos and M. Frodigh, "Realizing the Tactile Internet: Haptic Communications over Next Generation 5G Cellular Networks," in IEEE Wireless Communications, vol. 24, no. 2, pp. 82-89, April 2017.

A. Barbato, C. Bolchini, M. Delfanti, A. Geronazzo, E. Quintarelli, V. Olivieri, C. Rottondi, G. Verticale, G.Accetta, A. Ded`e, G. Massa, M. Trioni, "An Energy Management Framework for Optimal Demand Response in a Smart Campus", in Proceedings of 4th International Conference on Green IT Solutions REEN, June 2015.

A. Gunasekaran and E. W. T Ngai, "Information systems in supply chain integration and management", Elsevier, European Journal of Operational Research, Volume 159, Issue 2, Pages 269-295, 1 December 2004.

A. M. M. Ali, N. M. Ahmad, A. H. M. Amin, "Cloudlet-based cyber foraging framework for distributed video surveillance provisioning", Information and Communication Technologies (WICT), 2014 Fourth World Congress on, Bandar Hilir, Malaysia, December 2014.

A. Orsino, G. Araniti, P. Scopelliti, I. A. Gudkova, K. E. Samouylov, A. Iera, "Optimal subgroup configuration for multicast services over 5G-satellite systems", in Proceedings of International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Cagliari, Italy, 7-9 June 2017.

A. P. Plageras, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, Byung-Gyu Kim, Brij Gupta, "Efficient Large-Scale Medical Data (eHealth Big Data) Analytics in Internet of Things", in Proceedings of 19th IEEE International Conference on Business Informatics (CBI'17), International Workshop on the Internet of Things and Smart Services (ITSS2017), 24-26 July 2017, Thessaloniki, Greece. [DOI: 10.1109/CBI.2017.3]

A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, B. B. Gupta, "Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings", Future Generation Computer Systems, vol. 82, pp. 349-357, May 2018. [DOI: 10.1016/j.future.2017.09.082]

Abbas Mardani, Mahyar Kamali Saraji, Arunodaya Raj Mishra, and Pratibha Rani, "A novel extended approach under hesitant fuzzy sets to design a framework for assessing the key challenges of digital health interventions adoption during the COVID-19 outbreak", Elsevier, Applied Soft Computing, Volume 96, November 2020.

Abhinav Kathuria, "Issues and Challenges in the Era of Big Data Mining", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, Issue 6, June 2016.

Ahmed E. Khaled and Sumi Helal, "Interoperable communication framework for bridging RESTful and topic-based communication in IoT", Future Generation Computer Systems, 92 (2019) 628-643.

Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow, "Digital Twin: Enabling Technologies, Challenges and Open Research", IEEE Access, Vol. 8, 2020, doi: 10.1109/ACCESS.2020.2998358.

Akhirul Islam, Arindam Debnath, Manojit Ghose, and Sucheana Chakraborty, "A Survey on Task Offloading in Multi-access Edge Computing", Elsevier, Journal of Systems Architecture, June 2021.

Anand, A. 2022. 5 Advantages of Using AI in Language Learning. [online] AnalyticSteps. Available at: https://www.analyticssteps.com/blogs/5-advantages-using-ai-language-learning.

Anass Sedrati and Abdellatif Mezrioui, “A Survey of Security Challenges in Internet of Things”, Advances in Science, Technology and Engineering Systems Journal (ASTES), Vol. 3, No. 1, pages: 274-280, 2018.

Andreas P. Plageras, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, “IoT-based Surveillance System for Ubiquitous Healthcare”, 42nd Annual Conference of the IEEE Industrial Electronics Society, 24/10/2016 - 27/10/2016.

Annie Gilda Roselin , Priyadarsi Nanda , Surya Nepal , Xiangjian He, and Jarod Wright, “Exploiting the remote server access support of CoAP protocol”, IEEE Internet of Things Journal, 2019. DOI: 10.1109/JIOT.2019.2942085.

Anurag, Sanaz Rahimi Moosavi, Amir-Mohammad Rahmani, Tomi Westerlund, Geng Yang, Pasi Liljeberg, and Hannu Tenhunen, “Pervasive Health Monitoring Based on Internet of Things: Two Case Studies”, Wireless Mobile Communication and Healthcare (Mobihealth), 2014 EAI 4th International Conference, Pages: 275-278, 2014.

Artika Arista, Khairun Nisa, and Meiah Ngafidin, “An Information System Risk Management of a Higher Education Computing Environment”, International Journal on Advanced Science, Engineering and Information Technology, Vol. 12 (2022) No. 2, pages: 557-564, DOI:10.18517/ijaseit.12.2.13953.

Asharul Islam Khan and Ali Al-Badi, “Open Source Machine Learning Frameworks for Industrial Internet of Things”, Elsevier, Science Direct, The 11th International Conference on Ambient Systems, Networks and Technologies (ANT), Procedia Computer Science 170 (2020) 571-577, April 6-9, 2020, Warsaw, Poland.

Atefeh Goshvarpour, Ataollah Abbasi, and Ateke Goshvarpour. “An accurate emotion recognition system using ECG and GSR signals and matching pursuit method”, Biomedical Journal, 2017.

B. Kim, K. E. Psannis, H. Bhaskar, “Special section on emerging multimedia technology for smart surveillance system with IoT environment”, The Journal of Supercomputing, Volume 73, Issue 3, pp 923–925, March 2017.

Baraa Mohammed Hassan and Haider K. Hoomod, “Comparative Study of Encryption Algorithms for Data Security in WoT and IoT”, Turkish Journal of Computer and Mathematics Education, Vol. 12, No. 12, pp 2722-2727, 2021.

C. Clavel, T. Ehrette, G. Richard, "Events Detection for an Audio-Based Surveillance System," in Proceedings of IEEE ICME International Conference on Multimedia and Expo, pp. 1306-1309, July 2005.

C. K. M. Lee, Y. Z. Huo, S. Z. Zhang, and K. K. H. NG, “Design of a Smart Manufacturing System With the Application of Multi-Access Edge Computing and Blockchain Technology”, IEEE Access, Vol. 8, February 2020.

C. Pacchierotti, S. Sinclair, M. Solazzi, A. Frisoli, V. Hayward and D. Prattichizzo, "Wearable Haptic Systems for the Fingertip and the Hand: Taxonomy, Review, and Perspectives," in IEEE Transactions on Haptics, vol. 10, no. 4, pp. 580-600, 1 Oct.-Dec. 2017.

C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, “Architecture for Security in IoT Environments”, in Proceedings of 26th IEEE International Symposium on Industrial Electronics, 19-21 June 2017, Edinburgh, Scotland, UK. [DOI: 10.1109/ISIE.2017.8001447]

C. Stergiou, K. E. Psannis, “Efficient and Secure Big Data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017.

C. Stergiou and K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley, International Journal of Network Management, pp. 1-12, May 2016.

C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, December 2016.

C. Stergiou, K. E. Psannis, B. Gupta, Y. Ishibashi, "Security, Privacy & Efficiency of Sustainable Cloud Computing for Big Data & IoT", Elsevier, Sustainable Computing, Informatics and Systems, vol. 19, pp. 174-184, September 2018.

C. Stergiou, K. E. Psannis, "Algorithms for Big Data in Advanced Communication Systems and Cloud Computing", in Proceedings of 19th IEEE Conference on Business Informatics 2017 (CBI2017), Doctoral Consortium, 24-26 July 2017, Thessaloniki, Greece.

Charilaos Akasiadis, Vassilis Pitsilis, and Constantine D. Spyropoulos, "A Multi-Protocol IoT Platform Based on Open-Source Frameworks", Sensors 2019, 19, 4217, DOI: 10.3390/s19194217.

Charles Wheelus and Xingquan Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework", MDPI, IoT Journal, 259-285, October 2020.

Chi-Hung Hsiao, Wei-Po Lee, "OPIOT: Design and Implementation of an Open Communication Protocol Platform for Industrial Internet of Things", Elsevier, Internet of Things Journal, 16 (2021) 100441, August 2021.

Christos L. Stergiou, Konstantinos E. Psannis, Brij B. Gupta, "IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network", IEEE Internet of Things Journal, Vol.8, No.7, April 2021.

Chunyang Hu, Jingchen Li, Haobin Shi, Bin Ning, and Qiong Gu, "Decentralized Offloading Strategies Based on Reinforcement Learning for Multi-Access Edge Computing", MDPI, Information 2021, 12, 343, https://doi.org/10.3390/info12090343

D. Agrawal, B. B. Gupta, S. Yamaguchi, K. E. Psannis, "Recent Advances in Mobile Cloud Computing", Wireless Communications and Mobile Computing, December 2017.

D. Tomtsis, S. Kontogiannis, G. Kokkonis, I. Kazanidis, S. Valsamidis, "Proposed cloud infrastructure of wearable and ubiquitous medical services", 5th Int. Conf. on Digital Information Processing and Communications (ICDIPC 2015), pp. 213-218, Switzerland, Oct. 2015.

Dan Wang, Dong Chen, Bin Song, Nadra Guizani, Xiaoyan Yu, and Xiaojiang Du, "From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies", IEEE Communications Magazie, October 2018.

Davide Borsatti, Gianluca Davoli, Walter Cerroni, and Carla Raffaelli, "Enabling Industrial IoT as a Service with Multi-Access Edge Computing", IEEE Communications Magazine, Networks for Cyber-Physical Systems and Industry 4.0, August 2021.

Designspark, "11 Internet of Things (IoT) Protocols You Need to Know About", 20 Apr 2015.

Dominik Martin, Niklas Kühl, and Marcel Schwenk, "Towards a Reference Architecture for Future Industrial Internet of Things Networks", 23rd IEEE Conference on Business Informatics (CBI), September 2021.

Dr. Sam Rizvi, Dr. Syed Zeeshan Hussain, and Neeta Wadhwa, “Performance Analysis of AES and TwoFish Encryption Schemes”, IEEE, 2011 International Conference on Communication Systems and Network Technologies.

Edielson P. Frigieri, Daniel Mazzer, and Luis F. G. Parreira, “M2M Protocols for IoT: A Comparison of Approaches”, SBrT2015, 1-4 De Setembro de 2015, Juiz de For a, MG.

Elias Yaacoub, Khalid Abualsaud, Tamer Khattab, Mohsen Guizani, and Ali Chehab, “Secure mHealth IoT Data Transfer from the Patient to the Hospital: A Three-Tiers Approach”, IEEE Wireless Communications, 2019. DOI: 10.1109/MWC.2019.1800590.

Emanuele Di Pascale, Irene Macaluso, Avishek Nag, Mark Kelly, Linda Doyle, “The Network as a Computer: a Framework for Distributed Computing over IoT Mesh Networks”, IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2018.2823978.

Enamul Kabir, Jiankun Hu, Hua Wang, Guangping Zhuo, A novel statistical technique for intrusion detection systems, Future Generation Computer Systems, 2017, ISSN 0167-739X.

F. Licandro, G. Schembra, "WirelessMesh Networks to Support Video Surveillance: Architecture, Protocol, and Implementation Issues", EURASIP Journal on Wireless Communications and Networking, no. 2007, pp. 1-13, January 2007.

Fabian Nack, Institute of Computer Science (ICS), “An Overview on Wireless Sensor Networks”, 2009.

Fahad Mira, “IoT security threats analysis based on components, layers and devices”, American Journal of Science and Engineering (AJSE) 2019, Vol. 1, Issue 1, 1-10.

G. Ding, Y. Guo, J. Zhou, Y. Gao, “Large-Scale Cross-Modality Search via Collective Matrix Factorization Hashing”, IEEE Transactions on Image Processing, vol. 25, no. 11, pp. 5427-5440, September 2016.

G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

G. Fettweis, “The Tactile Internet: Applications and Challenges,” IEEE Veh. Technol. Mag., vol. 9, no. 1, pp. 64–70, March 2014.

G. Kokkonis, G. Minopoulos, K. E. Psannis & Y. Ishibashi, “Evaluating Vibration Patterns in HTML5 for Smartphone Haptic Applications,”. In 2019 2nd World Symposium on Communication Engineering (WSCE) pp. 122-126, December 2019. IEEE.

G. Kokkonis, K. E. Psannis, M. Roumeliotis and D. Schonfeld, “Real-time wireless multisensory smart surveillance with 3D-HEVC streams for internet-of-things (IoT)”, Journal of Supercompuitng, Volume 73, Issue 3, pp 1044–1062, March 2017.

G. Kokkonis, K. Psannis, M. Roumeliotis, S. Kontogiannis, "A Survey of Transport Protocols for Haptic Applications," 16th Panhellenic Conference on Informatics with international participation (PCI 2012), Greece, Oct. 2012.

G. Kokkonis, K.E. Psannis, M. Roumeliotis, "Network Adaptive Flow Control Algorithm for Haptic Data Over the Internet–NAFCAH", Book chapter of Genetic and Evolutionary Computing, pp. 93-102, Sept. 2015.

G. Kokkonis, S. Kontogiannis, D. Tomtsis, "An Open Source Architecture of a Wireless Body Area Network in a Medical Environment", Int. Journal of Digital Information and Wireless Communications (IJDIWC), vol. 6, no. 2, Apr. 2016.

G. Lilis, G. Conus, N. Asadi, M. Kayal, “Towards the next generation of intelligent building: An assessment study of current automation and future IoT based systems with a proposal for transitional design”, Sustainable Cities and Society, vol 28, pp. 473-481, January 2017.

G. Minopoulos, G. Kokkonis, K. E. Psannis & Y. Ishibashi, “A Survey on Haptic Data Over 5G Networks,” International Journal of Future Generation Communication and Networking, vol. 12, no. 2, pp. 37-54, 2019.

G. Skourletopoulos, C. X. Mavromoustakis, G. Mastorakis, J. Mongay Batalla and J. N. Sahalos, “An Evaluation of Cloud-Based Mobile Services with Limited Capacity: A Linear Approach”. Soft Computing journal (2016).

Garg SK, Versteeg S, Buyya R. “A framework for ranking of cloud computing services”. Future Generation Computer Systems. 2013;29(4):1012–1023.

Georgios Lilis, Gilbert Conus, Nastaran Asadi, and Maher Kayal, “Towards the next generation of intelligent buildings: An assessment study of current automation and future IoT-based systems with a proposal for transitional design”, Sustainable Cities and Society, 2016.

Getenet Tefera, Kun She, Maya Shelke, and Awais Ahmed, “Decentralized adaptive resource-aware computation offloading & caching for multi-access edge computing networks”, Elsevier, Sustainable Computing: Informatics and Systems, 30 (2021) 100555.

H. Detmold, A. van den Hengel, A. Dick, A. Cichowski, R. Hill, E. Kocadag, K. Falkner, D. S. Munro, "Topology Estimation for Thousand-Camera Surveillance Networks", in Proceedings of First ACM/IEEE International Conference on Distributed Smart Cameras, ICDSC '07, Adelaide, Australia, September 2007.

Haixia Peng and Xuemin Shen, “Deep Reinforcement Learning Based Resource Management for Multi-Access Edge Computing in Vehicular Networks”, IEEE Transactions on Network Science and Engineering, Vol. 7, No. 4, October-December 2020.

Hamid Al-Hamadi and Ray Chen, “Trust-Based Decision Making for Health IoT Systems”, IEEE Internet of Things Journal, Vol. 4, No. 5, October 2017.

Hanane Lamaazi, Nabil Benamar, and Antonio J Jara, “RPL-based networks in static and mobile environment: A performance assessment analysis”, Journal of King Saud University – Computer and Information Sciences, 30 (2018) 320-333.

Harikrishna Pydi and Ganesh Neelakanta Iyer, “Analytical Review and Study on Load Balancing in Edge Computing Platform”, IEEE, Fourth International Conference on Computing Methodologies and Communication (ICCMC 2020).

Hatem Ben Sta, Quality and the efficiency of data in “Smart-Cities”, Future Generation Computer Systems, Volume 74, 2017, Pages 409-416, ISSN 0167-739X.

Hamid Al-Hamadi and Ray Chen, “Trust-Based Decision Making for Health IoT Systems”, IEEE Internet of Things Journal, Vol. 4, No. 5, October 2017.

Heng Wang, Daijin Xiong, Ping Wang, and Yuqiang Liu, “A Lightweight XMPP Publish/Subscribe Scheme for Resource-Constrained IoT Devices”, IEEE Access, 2017. DOI: 10.1109/ACCESS.2017.2742020.

Hilbert, M., & López, P. (2011). The World’s Technological Capacity to Store, Communicate, and Compute Information. Science, 332(6025), 60–65. doi:10.1126/science.1200970.

Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson, “The industrial internet of things (IIoT): An analysis framework”, Elsevier, Computers in Industry, 101 (2018), 1-12.

Hui Zhou, Changyang She, Yansha Deng, Mischa Dohler, and Arumugam Nallanathan, “Machine Learning for Massive Industrial Internet of Things”, arXiv:2103.08308v1 [cs.LG] 10 March 2021.

Hung Cao, "Technical Report: What is the next innovation after the Internet of Things?", People in Motion Lab (Cisco Big Data Analytics), Department of Geodesy and Geomatics Engineering, University of New Brunswick, 2017.

I. Heđi, I. Špeh, A. Šarabok, “IoT network protocols comparison for the purpose of IoT constrained networks”, MIPRO 2017, May 22- 26, 2017, Opatija, Croatia.

I. Romdahani I. Romdhani, A. Y. Al-Dubai, M. Qasem, B. Ghaleb, I. Wadhaj, “Cooja Simulator Manual”, Technical Report, Edinburgh Napier University, July 2016.

IEEE P1918 Tactile Internet Emerging Technologies Subcommittee. Available: http://ti.committees.comsoc.org

Internet Society, “The Internet of Things: An Overview”. INTERNETSOCIETY.ORG, October 2015.

J. Basnayake, R. Amarasinhe, R. Attalage, T. Udayanga, B. Jayasekara, “Artificial Intelligence Based Smart Building Automation Controller for Energy Efficiency Improvements in Existing Buildings”, International Journal of Advanced Information Science and Technology (IJAIST), vol. 40, No. 40, August 2015.

J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

J. L. Hernandez-Ramos, M. V. Moreno, J. B. Bernabe, D. G. Carrillo, A. F. Skarmeta, “SAFIR: Secure access framework for IoT-enabled services on smart buildings”, Journal of Computer and System Sciences, vol. 81, issue: 8, pp. 1452-1463, December 2015.

J. Li, H. Yang, L. Chen, J. Li, C. Zhi, “An end-to-end generative adversarial network for crowd counting under complicated scenes”, in Proceedings of International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Cagliari, Italy, 7-9 June 2017.

J. Li, L. Huang, Y. Zhou, S. He, Z. Ming, "Computation partitioning for mobile cloud computing in big data environment", IEEE Transactions on Industrial Informatics, Vol. 11 January 2017.

J. Shah, B. Mishra, “Customized IoT Enabled Wireless Sensing and Monitoring Platform for Smart Buildings”, Procedia Technology, vol. 23, pp. 256-263, February 2016.

Jordi Mongay Batalla and Piotr Krawiee, “Conception of ID layer performance at the network level for the Internet of Things”, Personal and Ubiquitous Computing, Vol. 18, Issue: 2, Pages: 465-480, February 2014.

Jose L. Hernandez-Ramos, M. Victoria Moreno, Jorge Bernal Bernabe, Dan Garcia Carrillo, and Antonio F. Skarmeta, “SAFIR: Secure Access Framework for IoT-enabled Services on Smart Buildings”, Journal of Computer and System Sciences, pages: 1452-1463, 2015.

Jun-Jie Yu, Mingxiong Zhao, Wen-Tao Li, Di Liu, Shaowen Yao, and Wei Feng, “Joint Offloading and Resource Allocation for Time-Sensitive Muli-Access Edge Computing Network”, 2020 IEEE Wireless Communications and Networking Conference (WCNC), Seoul, Korea (South), June 2020.

Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions”, IEEE Communication Magazine, January 2017.

K. Antonakoglou, X. Xu, E. Steinbach, T. Mahmoodi and M. Dohler, "Toward Haptic Communications Over the 5G Tactile Internet," in IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3034-3059, Fourthquarter 2018.

K. E. Psannis, S. Xinogalos, and A. Sifaleras, “Convergence of Internet of Things and Mobile Cloud Computing”, Systems Science & Control Engineering (An open access journal), Vol. 14, No. 1, Pages: 476-483, Department of Applied Informatics, School of Information Sciences, University of Macedonia, Greece, 2014. http://www.tandfonline.com/doi/full/10.1080/21642583.2014.913213

K. Lin, M. Chen, J. Deng, M. M. Hassan, G. Fortino, “Enhanced Fingerprinting and Trajectory Prediction for IoT Localization in Smart Buildings”, IEEE Transactions on Automation Science and Engineering, vol. 13, issue: 3, pp. 1294-1307, April 2016.

Kai-Hsiang Liu and Wanjiun Liao, “Intelligent Offloading for Multi-Access Edge Computing: A New Actor-Critic Approach”, IEEE, ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7-11 June 2020.

Kalliopi Kyriakou, Bernd Resch, Günther Sagl, Andreas Petutschnig, Christian Werner, David Niederseer, Michael Liedlgruber, Frank Wilhelm, Tess Osborne, and Jessica Pykett. “Detecting Moments of Stress from Measurements of Wearable Physiological Sensors”, Article in Sensors, September 2019.

Khalid Haseeb, Ikram Ud Din, Ahmad Almogren, Imran Ahmed, and Mohsen Guizani, “Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things”, Elsevier, Sustainable Cities and Society Journal, 68 (2021) 102779.

Kosmas Alexopoulos, Spyros Koukas, Nikoletta Boli, and Dimitris Mourtzis, “Architecture and development of an Industrial Product Service Systems”, Elsevier, Science Direct, 51st CIRP Conference on Manufacturing Systems, Procedia CIRP 72 (2018), 880-885.

L. Berntzen, M. R. Johannessen, A. Florea, “Sensors and the Smart City: Creating a Research Design for Sensor-based Smart City Projects”, in Proceedings of 5th International Conference on Smart Cities, Systems, Devices and Technologies (SMART 2016), Valencia, Spain, May 2016.

L. D. Xu, W. He, S. Li, “Internet of Things in Industriew: A Survey”, IEEE Transactions on Industrial Informatics, vol. 10, no. 4, November 2014.

Lin Shi, Shah Nazir, Liquan Chen, and Rui Zhu, “Secure convergence of artificial intelligence and internet of things for cryptographic cipher-a decision support system”, Springer, Multimedia Tools and Applications (2021) 80:31451-31463.

Lixiong Leng, Jingchen Li, Haobin Shi, and Yi'an Zhu, "Graph convolutional network-based reinforcement learning for tasks offloading in multi-access edge computing", Springer, Multimedia Tools and Applications (2021) 80:29163-29175, https://doi.org/10.1007/s11042-021011130-5.

Ljubomir M. Vracar, Milan D. Stojanovic, Aleksandar S. Stanimirovic, and Zoran D. Prijic, "Influence of Encryption Algorithms on Power Consumption in Energy Harvesting Systems", Hindawi, Journal of Sensors, Volume 2019.

Luca Catarinucci, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone, "An IoT-Aware Architecture for Smart Healthcare Systems", IEEE Internet of Thing Journal, Vol. 2, No. 6, December 2015, DOI 10.1109/JIOT.2015.2417684.

M. J. Kaur, P. Matheshwari, "Building Smart Cities Applications using IoT and Cloud-based Architectures", in Proceedings of 2016 International Conference on Industrial Informatics and Computer Systems (CIICS), 13-15 March 2016, Sharjah, United Arab Emirates.

M. Mahalingam, "Challenges in Industrial Internet of Things", International Journal of Exclusive Global Research, Vol. 6, Issue: 8, August 2021.

M.-P. Hosseini, D. Pompili, K. Elisevich, H. Soltanian-Zadeh, "Optimized Deep Learning for EEG Big Data and Seizure Prediction BCI via Internet of Things", IEEE Transactions on Big Data, vol. 3, issue: 4, pp. 392-404, December 2017.

M. Simsek, A. Aijaz, M. Dohler, J. Sachs and G. Fettweis, "The 5G-Enabled Tactile Internet: Applications, requirements, and architecture," 2016 IEEE Wireless Communications and Networking Conference, Doha, 2016, pp. 1-6.

M. V. Moreno, L. Dufour, A. F. Skarmeta, A. J. Jara, D. Genoud, B. Ladevie, J.-J. Bezian, "Big data: the key to energy efficiency in smart buildings", Soft Computing, vol. 20, issue: 5, pp. 1749-1762, May 2016.

Maha Alqallaf, "Towards a Safe and Secure Internet of Things Critical Infrastructure", International Journal of Computer Science and Information Security (IJCSIS), Vol. 19, No. 2, February 2021.

Mario Frustaci, Pasquale Pace, Gianluca Aloi, and Giancarlo Fortino, "Evaluating critical security issues of the IoT world: Present and Future challenges", IEEE Internet of Things Journal, 2017.

Md. Shirajum Munir, Sarder Fakrul Abedin, Do Hyeon Kim, and Nguyen H. Tran, "A Multi-Agent System Toward the Green Edge Computing with Microgrid", IEEE Xplore, 2019.

Media Aminian and Hamid Reza Naji, "A Hospital Healthcare Monitoring System Using Wireless Sensor Networks", Journal on Health and Medical Informatics, Vol. 4, Issue: 2, 2013.

Min Chen, Shiwen Mao, and Yunhao Liu, "Big Data: A Survey", Mobile Network Applications, Vol. 19, Pages: 171-209, 2014.

Mingqiang Zhu, Liu Chang, Nan Wang, and Ilsun You, "A Smart Collaborative Routing Protocol for Delay Sensitive Applications in Industrial IoT", IEEE Access, 2020. DOI: 10.1109/ACCESS.2017.

Mirjana Maksimovic, Vladimir Vujovic and Branko Perisic, "A Custom Internet of Things Healthcare System", 10th Iberian Conference on Information Systems and Technologies (CISTI), Pages: 1-6, June 2015.

Michele Amoretti, Riccardo Pecori, Yanina Protskaya, Luca Veltri, and Francesco Zanichelli, “A Scalable and Secure Publish/Subscribe-Based Framework for Industrial IoT”, IEEE Transactions on Industrial Informatics, Vol. 17, No. 6, June 2021.

Mohammad Haghighat et al, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," Expert Systems with Applications, vol. 11, no. 42, pp. 7905-7916, 30/11/2015.

Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham, and Mohamed Marwan, “A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention”, Symbiosis, Journal of Computer Science Applications and Information Technology, 2018.

Moshaddique Al Ameen and Kyung-sup Kwak, “Social Issues in Wireless Sensor Networks with Healthcare Perspective”, The International Arab Journal of Information Technology, Vol. 8, No. 1, January 2011.

Naveen Kolhe and Nikhat Raza, “Throughput Comparison Results of Proposed Algorithm with Existing Algorithm”, The International Journal of Engineering and Science (IJES), Vol. 2, Issue 12, pp 92-98, 2013.

NGMN Alliance, NGMN 5G White Paper, https://www.ngmn.org/uploads/media/NGMN 5G White Paper V1 0.pdf, February 2015.

Nitin Naik, “Choice of Effective Messaging Protocols for IoT Systems: MQTT, CoAP, AMQP and HTTP”, IEEE, 2017.

Nuzhat Khan, Nazmus Sakib, Ismot Jerin, Shaela Quader, and Amitabha Chakrabarty, “Performance Analysis of Security Algorithms for IoT devices”, 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), 21-23 Dec 2017, Dhaka, Bangladesh.

P. Chatterjee, R. Armentano, "Internet of Things for a Smart and Ubiquitous eHealth System", in Proceedings of IEEE Computational Intelligence and Communication Networks (CICN), International Conference on, December 2015.

P. K. Choubev, S. Pateria, A. Saxena, V. P. Chirayil SB, K. K. Jha, S. Basaiah PM, “Power Efficient, Bandwidth Optimized and Fault Tolerant Sensor Management for IOT in Smart Home”, Advance Computing Conference (IACC), 2015 IEEE International, 12-13 June 2015, Banglore, India.

Pandesswaran C., Surender S., and Karthik KV. “Remote Patient Monitoring System Based Coap in Wireless Sensor Networks”, International Journal of Sensor Networks and Data Communications, Vol. 5, No. 3, 2016.

Pankaj Dutta, Tsan-Ming Choi, Surabhi Somani, and Richa Butala, “Blockchain technology in supply chain operations: Applications, challenges and research opportunities”, Elsevier, Transportation Research Part E: Logistics and Transportation Review, Volume 142, October 2020.

Paridhika Kayal and Harry Perros, “A Comparison of IoT application layer protocols through a smart parking implementation”, 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Computer Science Department, North Carolina State University.

Priyanka Thota and Yoohwan Kim, “Implementation and Comparison of M2M Protocols for Internet of Things”, IEEE, 2016 4th Intl Conf on Applied Computing and Information Technology. DOI 10.1109/ACIT-CSII-BCD.2016.20.

Qing Fan, Jianhua Chen, Lazarus Jegatha Deborah, and Min Luo, “A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain”, Elsevier, Journal of Systems Architecture 117 (2021) 102112.

R. Yu, X. Huang, J. Kang, J. Ding, S. Maharjan, S. Gjessing, Y. Zhang, "Cooperative Resource Management in Cloud-Enabled Vehicular Networks", IEEE Transactions on Industrial Informatics, volume: 62, Issue: 12, pp 7938 - 7951, September 2015.

Raghav Toshniwal, Kanishka Ghish Dastidar, and Asoke Nath, “Big Data Security Issues and Challenges”, International Journal of Innovative Research in Advanced Engineering (IJIRAE), Issue: 2, Vol. 2, February 2015.

Rachit, Shobha Bhatt, and Prakash Rao Ragiri, “ Security Trends in Internet of Things: a survey”, Springer Nature Jurnal, Applied Sciences, (2021), 3:121.

Rakesh Kumar Lenka, Amiya Kumar Rath, and Suraj Sharma, “Building Reliable Routing Infrastructure for Green IoT Network”, IEEE Access, 2019, DOI:10.1109/ACCESS.2019.2939883.

Rana M Pir, “Security improvement and Speed Monitoring of RSA Algorithm”, International Journal of Engineering Development and Research (IJEDR), Volume 4, Issue 1, 2016.

Randeep Kaur & Supiya Kinger, "Analysis of Security Algorithms in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, 1/3/2014.

Reena Singh and Kunver Arif Ali, “Challenges and Security Issues in Big Data Analysis”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 5, Issue 1, January, 2016.

S. Alletto, R. Cucchiara, G. Del Fiore, L. Mainetti, V. Mighali, L. Patrono, G. Serra, “An Indoor Location-aware System for an IoT-based Smart Museum”, IEEE Internet of Things Journal, vol. 3, issue: 2, pp. 244-253, December 2015.

S. Dutt, A. Kalra, "A Scalable and Robust Framework for Intelligent Real-time Video Surveillance", Department of Electronics Engineering, Indian Institute of Technology (BHU), Varanasi, India, 2016.

S. Jeon, J.-S. Han, R. Shrestha, S. I. Park, H.K. Mok, H. M. Kim, J.-S. Seo, “MIMO Cloud Transmission Based on BICM-ID for High Data Rate Local Contents Delivery”, IEEE Transactions on Broadcasting, vol. 61, issue: 4, pp. 580-589, December 2015.

S. Kontogiannis, G. Kokkonis, S. Valsamidis, "Proposed Transport Protocols Suite for Wireless Medical Body Area Networks", International Journal of Next-Generation Networks (IJNGN) Vol.8, No.1, March 2016.

S. M. A. Oteafy and H. S. Hassanein, "Leveraging Tactile Internet Cognizance and Operation via IoT and Edge Technologies," in Proceedings of the IEEE, vol. 107, no. 2, pp. 364-375, Feb. 2019.

S. M. Riazul Islam, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. “The Internet of Things for Healthcare: A Comprehensive Survey”, IEEE Access, Vol. 3, Pages: 678-708, June 2015.

S. O. Ajiboye, P. Birch, C. Chatwin, R. Young, "Hierarchical Video Surveillance Architecture - A Chassis for Video Big Data Analytics and Exploration", in Proceedings of SPIE - The International Society for Optical Engineering, Falmer-Brighton, United Kingdom, February 2015.

S. Veluru, Y. Rahulamathavan, B. B. Gupta, M. Rajarajan, "Privacy Preserving Text Analytics: Research Challenges and Strategies in Name Analysis," Book on Securing Cloud-Based Databases with Biometric Applications, IGI-Global's Advances in Information Security, Privacy, and Ethics (AISPE) series, 2014.

Samer Jaloudi, "Communication Protocols of an Industrial Internet of Things Environment: A Comparative Study", MDPI, Journal, Future Internet 2019, 11, 16.

Sean Pham, Danny Yeap, Gisela Escalera, Rupa Basu, Xiangmei Wu, Nicholas J. Kenyon, Irva Hertz-Picciotto, Michelle J. Ko, and Cristina E. Davis. "Wearable Sensor System to Monitor Physical Activity and the Physiological Effects of Heat Exposure", Article in Sensors, February 2020.

Sha Zhu, Kaoru Ota, and Mianxiong Dong, "Green AI for IIoT: Energy Efficient Intelligent Edge Computing for Industrial Internet of Things", IEEE Transactions on Green Communications and Networking, 2473-2400, 2021.

Shahab Tayeb, Shahram Latifi, and Yoohwan Kim, "A Survey on IoT Communication and Computation Frameworks: An Industrial Perspective", IEEE Xplore, 978-1-5090-4228-9/17, 2017.

Shancang Li, Shanshan Zhao, Geyong Min, Lianyong Qi, and Gang Liu, "Lightweight Privacy-Preserving Scheme using Homographic Encryption in Industrial Internet of Things", IEEE Internet of Things Journal, 2327-4662, 2021.

Somchanok Tivatansakul and Michiko Ohkura. "Emotion Recognition using ECG Signals with Local Pattern Description Methods", International Journal of Affective Engineering, 2015.

Sotirios K. Goudos, Panagiotis I. Dallas, Stella Chatziefthymiou, Sofoklis Kyriazakos, "A Survey of IoT Key Enabling and Future Technologies: 5G, Mobile IoT, Sematic Web and Applications", Springer, Wireless Personal Communications, July 2017.

Sun Mao, Supeng Leng, Sabita Maharjan, and Yan Zhang, "Energy Efficiency and Delay Tradeoff for Wireless Powered Mobile-Edge Computing Systems With Multi-Access Schemes", IEEE Transactions on Wireless Communications, Vol. 19, No. 3, March 2020.

Sunita Sahu and Yugchhaya Dhote, "A Study on Big Data: Issues, Challenges and Applications", International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), 2016.

Syed Husain, Andreas Kunz, Athul Prasad, Konstantinos Samdanis, and JaeSeung Song, "Mobile Edge Computing with Network Resource Slicing for Internet of Things", 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, February 2018.

T. McGinley, "A morphogenetic architecture for intelligent buildings", Journal of Intelligent Buildings International, vol. 7, issue: 1, pp. 4-15, November 2014.

Taher M. Ghazal, "Internet of Things with Artificial Intelligence for Health Care Security", Springer, Arabian Journal for Science and Engineering, Research Article, Special Issue on Frontiers in Parallel Programming Models for Fog and Edge Computing Infrastructures, August 2021.

Team, K., 2022. Keras documentation: About Keras. [online] Keras.io. Available at: https://keras.io.

Tetsuya Yokotani and Yuya Sasaki, "Comparison with HTTP and MQTT on Required Network Resources for IoT", 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC).

"The NIST Definition of Cloud Computing", National Institute of Standards and Technology, Retrieved 24 July 2011.

Tie Li, Junyou Yang, and Dai Cui, “Artificial-intelligence-based algorithms in multi-access edge computing for the performance optimization control of a benchmark microgrid”, Elsevier, Physical Communication, 44 (2021) 101240.

Tsan-Ming, Choi,Stein, W. Wallace, and Yulan Wang, “Big Data Analytics in Operations Management”, Wiley Online Library, Production and Operations Management, Special Issue on Big Data in Supply Chain Management, Volume27, Issue10, Pages 1868-1883, October 2018.

Tuan Nguyen Gia, Amir-Mohammad Rahmani, Tomi Westerlund, Pasi Liljeberg, and HannuTenhunen, “Fault Tolerant and Scalable IoT-based Architecture for Health Monitoring”, Sensors Applications Symposium (SAS), Pages: 1-6, 2015 IEEE, June 2015.

U. L. N. Puvvadi, K. Di Benedetto, A. Patil, K.-D. Kang, Y. Park, "Cost-Effective Security Support in Real-Time Video Surveillance", IEEE Transactions on Industrial Informatics, Volume: 11, Issue: 6, pp 1457 - 1465, December 2015.

Udit Satija, Barathram Ramkumar, and M. Sabarimalai Manikandan, “Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring”, IEEE Internet of Things Journal, Vol. 4, No. 3, June 2017.

V. Moreno, M. A. Zamora, A. F. Skarmeta, “A Low-Cost Indoor Localization System for Energy Sustainability in Smart Buildings”, IEEE Sensors Journal, vol. 16, issue: 9, pp. 3246-3262, February 2016.

Vijayakannan Sermakani, Robert Bosch Engineering and Business Ltd, Project Management Practitioners, Conference 2014, Architecting Project Management for transforming lives, “Transforming healthcare through Internet of Things”, November 20th – 22nd, Thu-Sat, 2014, Nimhans Convention Center, Bangalore.

W. Lee, S. Cho, P. Chu, H. Vu, S. Helal, W. Song, Y.-S. Jeong, K. Cho, “Automatic agent generation for IoT-based smart house simulator”, Neurocomputing, vol. 209, pp. 14-24, October 2016.

W. Zhang, S. S. Cheung, M. Chen, "Hiding Privacy Information in Video Surveillance System", in Proceedings of IEEE ICIP International Conference on Image Processing, September 2005

Wahyono, A. Filonenko, K.-H. Jo, "Unattended Object Identification for Intelligent Surveillance Systems Using Sequence of Dual Background Difference" IEEE Transactions on Industrial Informatics, Volume: 12, Issue: 6, pp 2247 - 2255, December 2016.

Wei Zhou, Yuqing Zhang, and Peng Liu. “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved”, IEEE Internet of Things Journal, 15 June 2018.

Wencheng Sun, Zhiping Cai, Yangyang Li, Fang Liu, Shengqun Fang, and Guoyan Wang, “Security and Privacy in the Medical Internet of Things: A Review”, Security and Communication Networks, Hindawi, Volume 2018, Article ID 5978636, 9 pages, 2018.

Wentao Shang, Qiuhan Ding, Alessandro Marianantoni, Jeff Burke, and Lixia Zhang, “Securing Building Management Systems Using Named Data Networking”, IEEE Network, May/June 2014.

Wissam Abbass, Zineb Bakraouy, Amine Baina, and Mostafa Bellafkih, “Classifying IoT security risks using Deep Learning algorithms”, IEEE, 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), Marrakesh, Morocco, 16-19 Oct. 2018.

X. Yang, X. Qian, T. Mei, “Learning salient visual word for scalable mobile image retrieval”, Journal of Pattern Recognition, vol. 48, no. 10, pp. 3093-3101, October 2015.

Xiaolin Fang, Junzhou Luo, Guangchun Luo, Weiwei Wu, Zhipeng Cai, and Yi Pan, “Big Data Transmission in Industrial IoT Systems with Small Capacitor Supplying Energy”, IEEE Transactions on Industrial Informatics, 2018.

Y. Liu, G. Shou, Y. Hu, Z. Guo, H. Li, F. P. Beijing, H. S. Seah, “Towards a smart campus: Innovative applications with WiCloud platform based on mobile edge computing”, in Proceedings of 12th International Conference on Computer Science and Education (ICCSE), Houston, TX, USA, 22-25 August 2017.

Y. Sun, T.-Y. Wu, G. Zhao, M. Guizani, “Efficient Rule Engine for Smart Building Systems”, IEEE Transactions on Computers, vol. 64, issue: 6, pp. 1658-1669, August 2014.

Y. Wang, D. He, L. Ding, W. Zhang, W. Li, Y. Wu, N. Liu, Y. Wang, “Media Transmission by Cooperation of Cellular Network and Broadcasting Network”, IEEE Transactions on Broadcasting, vol. 63, issue: 3, pp. 571-576, September 2017.

Y. Ye, S. Ci, A. K. Katsaggelos, Y. Liu, Y. Qian, “Wireless Video Surveillance: A Survey”, IEEE Access, vol. 1, pp. 646-660, September 2013.

Yogesh Kumar, Rajiv Munjal and Harsh Sharma,”Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

Yunsick Sung, “RSSI-Based Distance Estimation Framework Using a Kalman Filter for Sustainable Indoor Computing Environments”, MDPI, Sustainability Journal, 8, 1136, 2016.

Yuang Chen and Thomas Kunz, “Performance Evaluation of IoT Protocols under a Constrained Wireless Access Network”, 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT).

Yuan Zhang, Limin Sun, Houbing Song, and Xiaojun Cao, “Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects”, IEEE Internet of Things Journal, Vol. 1, No. 4, August 2014.

Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things”, IEEE Internet of Things Journal, 2016.

Yuyi Mao, Changsheng You, Jun Zhang, Kaibin Huang, and Khaled B. Letaief, “A Survey on Mobile Edge Computing: The Communication Perspective”, IEEE Communications Surveys & Tutorials, Vol.19, No.4, Fourth Quarter 2017.

Y. Wang, D. He, L. Ding, W. Zhang, W. Li, Y. Wu, N. Liu, Y. Wang, “Media Transmission by Cooperation of Cellular Network and Broadcasting Network”, IEEE Transactions on Broadcasting, vol. 63, issue: 3, pp. 571-576, September 2017.

Z. Lin, G. Ding J. Han, J. Wang, “Cross-View Retrieval via Probability-Based Semantics-Preserving Hashing”, IEEE Transactions on Cybernetics, vol. PP, no.99, pp.1-14, September 2016.

Zeesha Mishra and Bibhudendra Acharya, “High throughput novel architectures of TEA family for high speed IoT and RFID applications”, Journal of Information Security and Applications, 61 (2021).

Zichao Zhao, Rui Zhao, Junjuan Xia, Xianfu Lei, Dong Li, Chau Yuen, and Lisheng Fan, “A Novel Framework of Three-Hierarchical Offloading Optimization for MEC in Industrial IoT Networks”, IEEE Transactions on Industrial Informatics, Vol. 16, No. 8, August 2020.

Zainab H. Ali and Hesham A. Ali, “Towards sustainable smart IoT applications architectural elements and design: opportunities, challenges, and open directions”, Springer, The Journal of Supercomputing, November 2020.

Zhangjie Fu et al, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, DOI: 10.1109/TPDS.2015.2506573, 2015.

Zhihan Lv and Liang Qiao, “AI-empowered IoT Security for Smart Cities”, ACM Transactions on Internet Technology, Vol. 21, No. 4, Article 99, July 2021.

Zhihan Lv, Liang Qiao, Amit Kumar Singh, and Qingjun Wang, “AI-empowered IoT Security for Smart Cities”, ACM Transactions on Internet Technology, Vol. 21, No. 4, Article 99, July 2021.

Appendix

Published Work in International Journals

Published Work 1

Algorithms for efficient digital media transmission over IoT and cloud networking

Authors: C. Stergiou, K. E. Psannis, **A. P. Plageras**, Y. Ishibashi, B.-G. Kim

Abstract: In recent years, with the blooming of Internet of Things (IoT) and Cloud Computing (CC), researchers have begun to discover new methods of technological support in all areas (e.g. health, transport, education, etc.). In this paper, in order to achieve a type of network that will provide more intelligent media-data transfer new technologies were studied. Additionally, we have been studied the use of various open source tools, such as CC analyzers and simulators. These tools are useful for studying the collection, the storage, the management, the processing, and the analysis of large volumes of data. The simulation platform which have been used for our research is CloudSim, which runs on Eclipse software. Thus, after measuring the network performance with CloudSim, we also use the Cooja emulator of the Contiki OS, with the aim to confirm and access more metrics and options. More specifically, we have implemented a network topology from a small section of the script of CloudSim with Cooja, so that we can test a single network segment. The results of our experimental procedure show that there are not duplicated packets received during the procedure. This research could be a start point for better and more efficient media data transmission.

Keywords: Cloud Computing, Internet of Things, Digital Media, Efficient Transmission, CloudSim, Contiki OS, Cooja.

I. INTRODUCTION

Cloud Computing consists a technology of internet services, providing remote use of hardware and software. As a result, the users of Cloud Computing could have access to information and data from any place at any time. In recent years, giant companies of the IT and software sectors investigate in survey the services of Cloud Computing.

Furthermore, another technology which generated relaying on Cloud Computing is Mobile Cloud Computing. Mobile Cloud Computing based on the concept of the “Cloud” and provides any type of information and data by no matter where and when, through mobile devices.

Particularly, Mobile Cloud Computing is defined as “the integration of Cloud Computing and Mobile technology in order to make any type of mobile devices resourceful in terms such as computational power, memory, storage and energy”. Regarding the usage of Cloud services in Mobile devices many types of services could be processed through it. Thus, high quality media could be transmitted through Cloud

environment progressed in applications which were installed and operated in Cloud. Considering this Mobile Cloud Computing, and also Cloud Computing in general, could be settled as a base technology to operate other technologies, such as Internet of Things, and consequently to be accomplished an integration of Cloud and IoT [1] [2] [3] [4] [5].

Internet of Things (IoT) is "a system of interrelated computing devices, mechanical and digital machines, objects that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction". Based on this definition, in IoT environments could be established transmission networks for information and data produced by applications running on it. Some examples of the possible application scenarios in Internet of Things would be the domotics, e-health, assisted living, and enhanced learning. Thus, all these could lead us to the conclusion that IoT can be used in order to operate applications that provide digital media [6] [7] [8] [9].

Digital media could be produced by surveillance video systems. In most cases, surveillance is used by people in order to influence, manage, direct, or protect them, by using sensors and cameras or other compatible devices.

Ordinarily, digital media format could be defined as the high quality video format produced by surveillance cameras. Those three aforementioned technologies could be combined and operate consolidated with the aim to have a more efficient network. This network would be based on Cloud and IoT environment, for transmitting high quality data, such as digital media [10] [11] [12] [13].

The rest of the paper is organized as follows. In section 2 there is a review of the related research in the area, which deals with the integration of Cloud and IoT, as these are used as a basis for data transmission. Section 3 presents and illustrates the simulation method of this work. In Section 4 demonstrated the simulation and the experimental results recorded. Finally, section 5 provides the conclusions of the current work and offers new possibilities for the development of future work.

II. RELATED REVIEW

In this section we present related works to our research. By studying the areas of collection, delivery, management, and analysis of large-scale data (Big Data), it is concluded that data centers are responsible for everyone since everything that happens to them will affect us all.

So in [14] is presented, through several open source platforms (e.g. Arduino), the implemented data center environmental monitoring system. The system's architecture design is the implementation key of success. With the implemented design and through the Internet we can identify in real-time the system logs and status. As an extension of that system is proposed the monitoring of real-time Big Data through HTML5 charts.

A region based approach is presented in [15], where Jun- Ho Huh and Kyungryong Seo discuss about efficient power consumption through the technologies

and techniques of Smart Grid. The main focus area of this research is the Programmable Logic Controller (PLC) technology in conjunction with power lines for the transmission of data in a network since it is an efficient and low-cost solution for efficient metering. The results from the analysis of the implemented PLC-based power-aware home network system design, using OPNET Modeler 14.5 PL8, were analyzed and compared to those of IEEE 802.11 WLAN MAC.
In another region based approach [16], a novel power- aware routing protocol is proposed. With this protocol and a mechanism which controls the delays, researchers maximize the lifetime of every node in an Ad-hoc network system. NS-2 was the simulator used for the verification of the network.

As is known, with the blooming of Big Data, the Cloud Computing (CC) also blossomed. However, there are open issues and challenges in this technology, for some of which are provided solutions by several researchers. In [17] there is an attempt to solve the problems of ignoring the content of multimedia and the difficulty in implementing solutions for the cloud platform. So, researchers proposed a new distributed multimedia programming model for its implementation on different service platforms and different multimedia applications. Also, an algorithm for decision making by users, based on local information, is also proposed.

One of the most challenging fields of Multi-clouds is the efficient workflow scheduling. So, in [18] researchers proposed an algorithm (Multi-Clouds Partial Critical Paths, MCPCPP) for Big data scheduling in Multi-clouds. This algorithm reduces the workflows' execution costs. At the same time, the algorithm indulges the determined restriction deadline. From the results it is concluded that the proposed algorithm is promising.

Moreover, in [19] researchers talk about the networking perspectives of three popular applications. These are YouTube, Facebook, and WhatchUp. Researchers analyzed the traffic and the network infrastructure which hosts these data flows. The DBStream platform was used to analyze the large amounts of data. Solutions for traffic monitoring, analysis, and services of cellular networks have also been proposed and discussed.

The Big Data are usually transmitted from the data production center to the remote environment so that it can be provided the analysis of these large amounts of data. The multiple bandwidth reservation requests issue is discussed with the use of a High-Performance Network (HPN) in which succeeded with the best average transmission. So, in [20] have been proposed two efficient and high-speed algorithms with polynomial time complexity. The algorithms were compared with two others and from the experimental results were both verified for their advanced performance.

The pervasive network services outstretch into ubiquitous computing environment. The users to get the services they need, they have to share personal and private information. To avoid the exposure to various attacks (eg. eavesdropping) researchers proposed in [21] a security scheme to secure the communications. The authentication scheme guarantees reliability and availability by securing the remote

access in Pervasive Computing Environment (PCE). The scheme provides security and convenience to the users.

III. SIMULATION METHOD

Based on previous works, with the aim to succeed a new type of network, which could provide more efficient data transmission a simulation tool was used. The simulation platform that used in this work is CloudSim. This simulation platform operates in the Eclipse environment, in java programming language. In CloudSim using the logic of a virtual system, and thus virtual management, we create Virtual Machines (VMs) [22] [23] [24] [25].

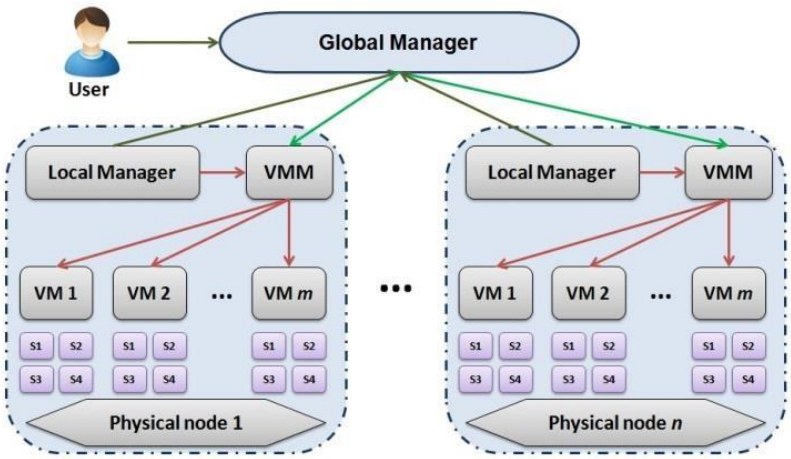


Fig. 1. Cloud System Model.

Figure 1 demonstrates how a user could interact through a Global Manager (application software) to a number of Cloud Virtual Machines. More specifically, each Cloud Virtual Machine consists of a Local Manager which interacts with a Virtual Machine Manager (VMM), and through the VMM established a communication path with the various individual VM devices. Each VM is connected to four sensors, from which it receives the data it then transmits to VMM. For each Cloud Virtual Machine there is a Physical Node which connects it to the network.

Table 1. Cloud Servers Configuration.

	Server Configuration 1	**Server Configuration 2**
Model	Dell PowerEdge T110	**HP ProLiant ML110 G5**
CPU Model	Intel E2160, 2C 1800MHz	**Intel Xeon 3075, 2C 2660MHz**
RAM	4GB	**4GB**
Network Bandwidth	1GB/sec	**1GB/sec**

Performance	1800 MIPS/core	**2660 MIPS/core**
Number of Servers Used	**400**	**400**

Table 1 lists the two types of Virtual Server Configuration for the Cloud which have been used for the simulation. In this work we used 400 Virtual Servers of the model Dell PowerEdge T110 and 400 Virtual Servers of the model HP ProLiant ML 110 G5.

Table 2. Power Consumption Information in Watt.

Consumption in %	**Dell PowerEdgeT110**	**HP ProLiant ML110G5**
0%	86	93.7
10%	89.4	97
20%	92.6	101
30%	96	105
40%	99.5	110
50%	102	116
60%	106	121
70%	108	125
80%	112	129
90%	114	133
100%	**117**	135

Table 2 depicts the rate of Watt Power Consumption from the information produced and transmitted from each type of Cloud Server, either Dell PowerEdge T110 or HP ProLiant G5. As we can observe, when the rate of consumption of watts increases, both the transmission of information increases.

Table 3. Virtual Machine Configuration.

	VM 1	**VM 2**	**VM 3**	**VM 4**
CPU Type	High-CPU medium instance	Extra Large instance	Small instance	Micro instance
Numberof Cores	1 Core	2 Cores	3 Cores	4 Cores
RAM	0.85GB	3.75GB	1.7GB	613MB
Network	1GB/sec	1GB/sec	1GB/sec	1GB/sec
Performance	2500 MIPS/core	2000 MIPS/core	1000 MIPS/core	500 MIPS/core

Table 3 shows the four types of VM that created and used for the simulation method. Each type had differentiated characteristics in order to be studied a wide range of results.

Table 4. Cloudlet Parameters.

Length (MB)	**File size (MB)**	**Output size (MB)**

5000	5000	5000

Table 4 demonstrates the Cloudlet Parameters which represent the volume of data used in a network in association with IoT technology. With the aim to proceed at a better simulate of high quality data, referring to digital data, we used large sizes in MB.

Subsequently, for further simulation procedure, we used Cooja Contiki simulator with the purpose of personalizing and extracting our network data in an environment with a defined topology.

IV. EXPERIMENTAL RESULTS

Having already tested the performance of the network we created in CloudSim, we perform a simulation in Cooja Contiki, where we tried to map the same network scenario, but also studied more aspects of this network. We implement a network topology of a small part of the previous scenario where examining a single network segment. Namely, we examined the communication and the efficiency of data transmission in a VMM, which includes in its range five VMs.

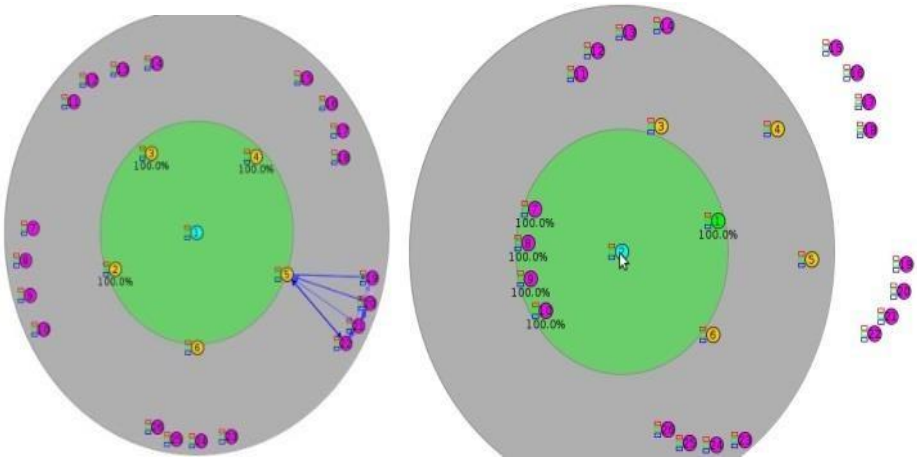
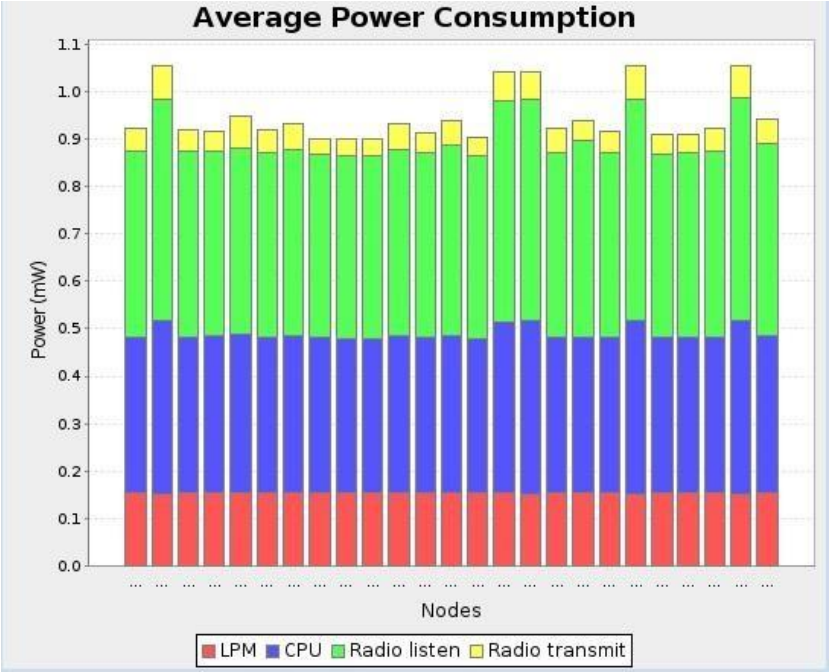


Fig. 2. Network Topology ([2a] and [2b]).

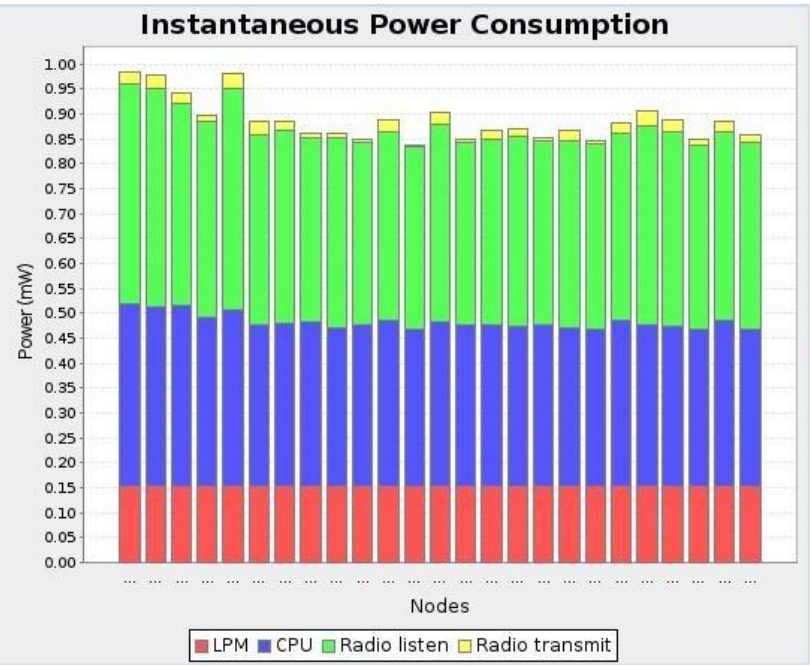
Figure 2a and Figure 2b show the topology of our proposed network. As we already mentioned, each separate part of our network consists of one VMM and five VMs. In each VM are connected four sensors. The range of the VMM contains only the five VMs, and the range of every VM contains only its four sensors. According to this, we observe that each VM contains only four sensors in its range, so as not to be inserted from the range of other VMs.

Figure 3 (a) and Figure 3 (b) demonstrates the Power Consumption of the Network. Figure 3 (a) demonstrates the average Power Consumption, where we can observe that LPM's power (red color) remains almost constant over time, as well as CPU's power (blue color). In contrast, the Radio listen's power (green color) and a little

less the Radio transmit's power (yellow color) where there is a greater variation in Power Consumption. Figure 3 (b) demonstrates the Instantaneous Power Consumption, where, same as before, we can observe that LPM's power (red color) remains almost constant over time, as well as CPU's power (blue color). And also, in contrast again, the Radio listen's power (green color) and a little less the Radio transmit's power (yellow color) where there is a greater variation in Power Consumption. In Instantaneous Power Consumption we observe that there is a big difference as regards the variation of the Radio transmit's power, compared with Average Power Consumption, as there are momentary fluctuations in the change in energy consumption during transmission.



(a) Average Power Consumption.



(b) Instantaneous Power Consumption

Fig. 3. Power consumption of the proposed network.

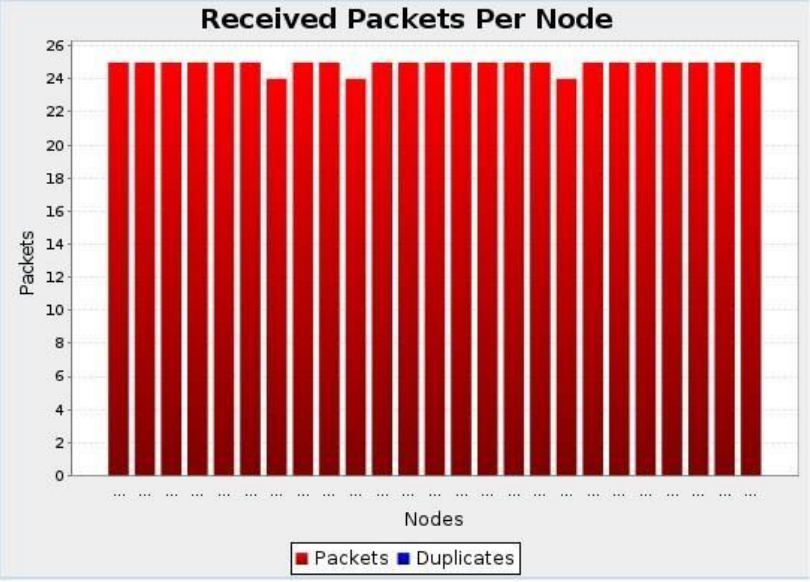


Fig. 4. Received Packets Per Node.

Figure 4 shows the transmitted packets which have been received per node. As we can observe, in most cases and almost every time all the nodes received the same number of packets. In addition to this, we can conclude that there are no duplicated packets received.

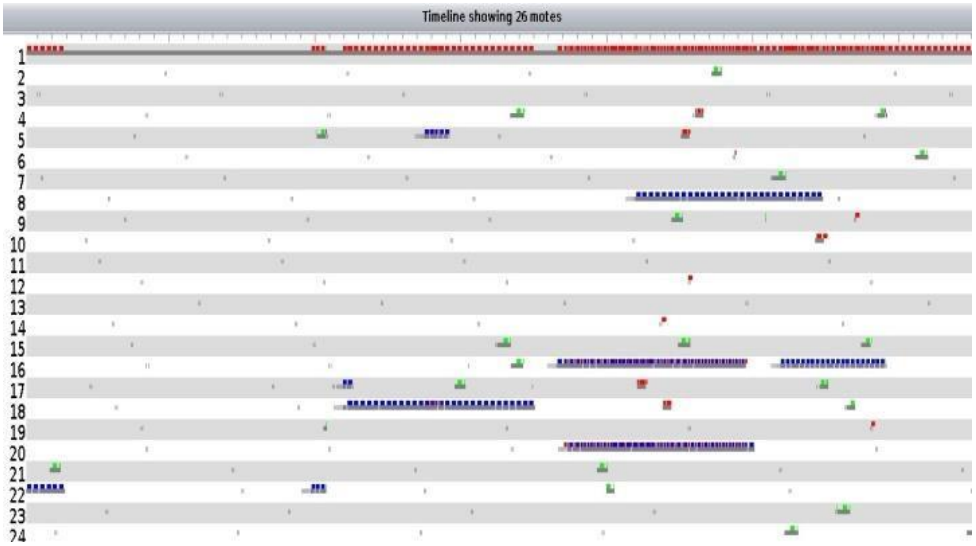


Fig. 5. Timeline showing the packets received per mote (node) over time.

Figure 5 demonstrates the packet transmission procedure through all the motes we used for the simulation in Contiki. With the word 'mote' is defined the node in 'Contiki language'. Through Figure 5, we can see that during the simulation process transmission, there are array packages with large size (large-scale data).

V. CONCLUSION

Due to the blooming of IoT in CC which takes part in the last years, the there is a need of discovering new methods of technological support in many sciences by the researchers. As part of these researches, in this work, with the aim to achieve a type of network that will provide more intelligent media-data transfer, we have studied new technologies, and the use of various open source tools, such as CC analyzers and simulators. Tool like these are useful for studying the collection, the storage, the management, the processing, and the analysis of large volumes of data. Furthermore, the simulation platform used is CloudSim and operates on Eclipse environment. Thus, after measuring the network performance with CloudSim, we use the Cooja emulator of the Contiki OS in order to confirm and access more metrics and options. As a result, we implemented a network topology from a small section of the script of CloudSim with Cooja, so that we can simulate a single network segment. The results of the experiment show that there are not duplicated packets received.

Finally, as future research, we suggest a further examination of the simulation analysis of the network performance in CloudSim simulator, and other simulation platforms, with the aim to have a better and improved contribution of the technology of Internet of Things with the additional 'help' of the Cloud Computing technology for the purpose of better transmission of high quality data. This research could be a start point for better and more efficient media data transmission.

REFERENCES

[1] M. Aazam, E.-N. Huh, M. St-Hilaire, C.-H. Lung, I. Lambadaris, "Cloud of Things: Integration of IoT with Cloud Computing" Springer, Robots and Sensor Clouds, vol. 36, pp. 77-94, August 2015.

[2] C. Stergiou, K. E. Psannis, B.-G. Kim, B. B. Gupta, "Secure integration of IoT and Cloud Computing", Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018.

[3] S. Sakr, A. Liu, D. M. Batista, M. Alomari, "A survey of large scale data management approaches in cloud environments", IEEE Communications Surveys & Tutorials, vol. 13, issue 3, pp. 311-336, April 2011.

[4] R. Kaur, S. Kinger, "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, issue. 3, pp. 171-176, March 2014.

[5] S. H. H. Madni, M. S. A. Latif, Y. Coulibaly, Shafi'i M. Abdulhamid, "Resource scheduling for infrastructure as a service (IaaS) in cloud computing: Challenges and opportunities", Journal of Network and Computer Applications, vol. 68, pp. 173-200, June 2016.

[6] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi,
B. B. Gupta, B.-G. Kim, "Architecture for security monitoring in IoT environments", in Proceedings of IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, Scotland (UK), 19-21 June, 2017.

[7] A. P. Plageras, C. Stergiou, G. Kokkonis, K. E. Psannis, Y. Ishibashi, B.-G. Kim, B. B. Gupta, "Efficient Large- scale Medical Data (eHealth Big Data) Analytics in Internet of Things", in Proceedings of 19th IEEE Conference on Business Informatics, International Workshop on Internet of Things and Smart Services, Thessaloniki, Greece, 24-26 July, 2017.

[8] C. Stergiou, K. E. Psannis, "Efficient and Secure Big Data delivery in Cloud Computing", Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017.

[9] F. Tao, Y. Cheng, L. D. Xu, L. Zhang, B. H. Li, "CCIoT- CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System", IEEE Transactions on Industrial Informatics, vol. 10, issue: 2, pp. 1435-1442, May 2014.

[10] M. Hilbert, P. López, "The World's Technological Capacity to Store, Communicate, and Compute Information", Science, vol. 332, issue: 6025, pp. 60-65, April 2011.

[11] A. P. Plageras, K. E. Psannis, Y. Ishibashi, B.-G. Kim, "IoT-based Surveillance System for Ubiquitous Healthcare", in Proceedings of IEEE 42nd Annual Conference of Industrial Electronics Society (IECON 2016), Florence, Italy, 23-26 October 2016.

[12] A. P. Plageras, C. Stergiou, K. E. Psannis, B.-G. Kim, B. B. Gupta, Y. Ishibashi, "Solutions for Inter- connectivity and Security in a Smart Hospital Building", in Proceedings of IEEE 15th International Conference on Industrial Informatics (INDIN), Emden, Germany, 24-26 July, 2017.

[13] C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley, International Journal of Network Management, vol. 27, issue: 3, pp. 1-12, May/June 2016.
[14] L. Nkenyereye, J. Jang, "Design of Data Center Environmental Monitoring System Based On Lower Hardware Cost", Journal of Multimedia and Information System, Vol. 3, No. 3, pp. 63-68, October 2016.
[15] J.-H. Huh, K. Seo, "PLC-Based Smart grid Home Network System Design and Implementation using OPNET Simulation", Journal of Multimedia and Information System, Vol. 1, No. 2, pp. 111-118, December 2014.
[16] J.-H. Huh, Y. Kim, K. Seo, "Power Aware Routing Protocol in Multimedia Ad-hoc Network Considering Hop Lifetime of Node", Vol. 1, No. 2, pp. 101-110, December 2014.
[17] M. Zheng, W. Wang, "Distributed Multimedia Scheduling in the Cloud", Journal of Multimedia and Information System, Vol. 2, No. 1, pp. 143-152, March 2015.
[18] P. Fiadino, P. Casas, A. D'Alconzo, M. Schiavone, A. Baer. "Grasping Popular Applications in Cellular Netwoks with Big Data Analytics Platform", IEEE Transactions on Network and Service Management, vol. 13, issue: 3, pp. 681-695, September 2016.
[19] B. Lin, W. Guo, N. Xiong, G. Chen, A. V. Vasilakos, H. Zhang. "A Pretreatment Workflow Scheduling Approach for Big Data Applications in Multi-cloud Environments", IEEE Transactions on Network and Service Management, vol. 13, issue: 3, pp. 681-695, September 2016.
[20] L. Zuo, M. M. Zhu, "Concurrent Bandwidth Reservation Strategies for Big Data Transfers in High- Performance Networks", IEEE Transactions on Network and Service Management, vol. 12, issue: 2, June 2015.
[21] B. Djellali, P. Lorenz, K. Balarbi, A. Chouarfia. "Security Model for Pervasive Multinedia Environment", Journal of Multimedia Information System, Vol. 1, No. 1, pp. 23-43, September 2014.
[22] Y. Chao-Tung, L. Jung-Chun, C. Shuo-Tsung, H. Kuan-Lung, "Virtual machine management system based on the power saving algorithm in cloud", Journal of Network and Computer Applications. vol. 80, pp. 165-180, February 2017.
[23] T. Fei, Y. Lei, L. Tianrui, D. Danting, "Energy efficiency of VM consolidation in IaaS clouds", The Journal of Supercomputing. Vol. 73, issue: 2, pp. 782- 809, February 2017.
[24] Q. Nguyen, T. Nam, T. "Minimizing Total Busy Time with Application to Energy-efficient Scheduling of Virtual Machines in IaaS clouds", in Proceedings of International Conference on Advanced Computing and Applications, pp. 141-148, Can Tho, Vietnam, 23-25 November 2016.
[25] B. Dinh-Mao, Y. YongIk, H. Eui-Nam, J. SungIk, "Energy efficiency for cloud computing system based on predictive optimization", Journal of Parallel and Distributed Computing, Vol. 102, pp. 103-114, April 2017.

Published Work in Book Chapters

Published Work 1

Secure Machine Learning scenario from Big Data in Cloud Computing via Internet of Things network

Authors: Christos Stergiou, **Andreas P. Plageras**, Kostas E. Psannis, and Brij B. Gupta

Abstract: The Cloud Computing (CC) technology refers to an infrastructure in which both data storage and data processing takes place outside the mobile device. Furthermore, another new and fast growing technology called Internet of Things (IoT) raises in the sector of networks and telecommunications with specifically concern in the 'modern' area of wireless telecommunications systems. Regarding our recent research, the main goal of the interaction and cooperation between things and objects sent through the wireless networks. It is to fulfill the objective set to them as a combined entity, with the aim to achieve a better environment for the use of Big Data (BD). In addition, count on the technology of wireless networks, both CC and IoT could be developed rapidly and together. In this paper, we survey IoT and Cloud Computing technologies with focus on security problems that both technologies faced. Particularly, these two aforementioned technologies (i.e Cloud Computing and IoT) have been compared, aiming to the familiar characteristics, and examined and discover the benefits of their integration focusing to secure the use and transmission of Big Data. Concluding, a contribution of CC and IoT technologies have been presented, and how the CC technology improves the operation of IoT as base technologies for Big Data systems.

Keywords: Internet of Things, Cloud Computing, Big Data, Security, Privacy

1 Introduction

"*Internet of Things*" (IoT) is a novel technology which operates in the sector of telecommunications. IoT could be defined by many researchers as "the network of devices, vehicles, buildings, and other items which are embedded with sensors, and there are connected to the network, permitting these objects to gather and interchange data" [1] [2] [3]. Over the next years, a flare in the number of connected devices as well as located sites, and the functions they will perform, are expected. Regarding the data used in a wireless network there are security and privacy issues that need to be addressed. The problem with security and data privacy in everyday life could be solved or could be minimized with the use of BD analysis tools and services. BD is a new popular term, used to describe the surprisingly rapid increase in the volume of data in structured and unstructured form [4] [5]. BD usually uses CC as a base technology in order to operate. Similar to this, another technology that could be used as a base technology is the Edge Computing (EC).

IoT could be settled as a type of network of physical objects or things which are embedded with software, electronics, sensors and connectivity that enables them. Due

to that, IoT achieves greater rate and service by transmitting data with operators and various inter-connected devices [6] [7] [8].

An approach has been made by researchers in [9], in order to help other researchers who are interested in security issues. This approach provides an IoT security analysis of the recent security research activity and a novel IoT framework that is validated through a case study. The authors of this paper have shown through their work that the evolution of autonomous objects raises security threats.

Thus, the need of "*cloud*" support has become inefficient due to the intensive computations, the mass storage, and the security issues. Some examples include limited storage capacity, communication capabilities, energy and processing. Inefficiencies like these have motivated us in order to find a model for the combination of CC and IoT. As a "*base*" technology, Cloud Computing consolidates various technologies and applications to get the maximum capacity and performance of the existing infrastructure [10] [11] [12].

On top of that, Mobile Cloud Computing (MCC) made its appearance, as a relative version of Cloud Computing, and it was improved by new developments in the field of "*Cloud Computing*". The latter aims provide access to data and information from anywhere at any time by obliterating the need for hardware equipment [2] [13] [14] [15]. More specifically, MCC is defined as an integration of cloud and mobile computing rendering mobile devices more resourceful. It is also a contemporary approach to innovative services for firms and institutions. CC can be used as a useful base for both Internet of Things and Video Surveillance technologies and provide improvements on their function [16] [17] [18].

Moreover, Cloud Computing aims to offer access to information and data from anywhere at any time, without the restrictions of the need for hardware equipment [11] [19] [20] [21]. As a result of the operations of CC, it could be used as a base technology for IoT and for several technologies in the telecommunications field, and could also provide improvements on their functions.

In addition to this, CC additionally used to be a base technology for other technologies due to its types of services [11] [21] [22]. One of those is the Big Data. BD is a term used to describe the expected, due to the connected to the Internet devices, rapid increase in the volume of data production. Subsequently, these large amounts of data could be defined as "*a broad term for data sets so large or complex that traditional data processing applications are inadequate*" [12] [21]. Furthermore, BD is often associated to the use of predictive analytics or certain advanced methods to extract knowledge from the data. Rarely, are also related to a particular size of set of data [4] [5]. Precision in BD could result in more confident decision making, and better decisions may drive in increased operational efficiency, reduced costs, and minimized risk [4]. From this scope, it can be observed that BD is now equally important both for business and internet. This happens because more information drives to more accurate analysis [11]. The real problem is not that the large amounts of data have been obtained, but whether they have any value or not. Hopefully, by predicting that organizations would be able to acquire information from any source, harness the relevant data, and analyze them in a specific way in order to get quick answers, the following should be achieved: 1) reduce costs, 2) reduce time, 3) produce new items and optimize their offerings, and 4) take more ingenious decisions [7].

Last but not least, since we are talking about BD, IoT, and CC/MCC many researchers tried to figure out ways for securing these sensitive/personal data. The security problems still remain a challenge since the new technologies are multiplied. Due to this, a security scheme for safe sensitive data transmission over the CC and the IoT devices has been proposed in [23]. Specifically, an alternative of RSA (Rivest-Shamir-Adleman) security has been deployed, namely MEMK ("*Memory Efficient Multi Key*") generation scheme, in order to provide support to the data transmitted from the IoT devices to the Cloud and back. This scheme has been also used by the authors of this paper [23] to boost the efficiency of the memory.

The rest of the paper is divided in sections as follows. Initially, in Section II has been presented a literature review related to the conjunction of the technologies mentioned in the introduction section (Section I) of the paper. Subsequently, in Section III there is an illustration of issues related with BD and their privacy. In Section IV has been

discussed in detail the field of IoT and some of its major functions. Moreover, in Section V the CC technology and its basic characteristics have been presented and analyzed. Section VI illustrates the integration of IoT and CC, and surveys some of the benefits of their integration. Finally, Section VII provides the conclusions of the current paper, and offers new possibilities for the development of future work.

2 Literature Review

To come through the proposed scenario various related works that discuss the combination of the three aforementioned technologies (Big Data, Cloud Computing and Internet of Things) have been studied. This section illustrates related work similar to this research. The main tumor of the related research studies is mainly related to previous work of our research team.

To start with, in [11] the authors aim in the interaction and the conjunction of Mobile Cloud Computing (MCC) and IoT through the integration of these technologies with the Big Data. This scenario, based on similar characteristics of MCC and IoT, and which of the benefits of these technologies could improve the use of BD applications. Also, in [6] an illustration has been presented of how the MCC and the IoT contribute to the BD technology, individually.

A region based research [2] presents a survey research of IoT and CC focusing on the issues based on data privacy of both technologies. Particularly, the authors of [2] try to combine these technologies with the purpose to find and examine the familiar characteristics and then discover the profits of their integration. Additionally, the authors illustrate the contribution of CC in the field of IoT, and through this it can be proved how the CC technology improves the operation of IoT.

In [7], the authors survey BD and CC technologies and their major features, focusing on security and data privacy issues. Particularly, a conjunction of the functionality of those two technologies has been done with the aim to consider the frequent characteristics, and in addition to this, to discover the profits which deal with security problems of their integration. Thus, a novel method of an algorithm has been presented in [7], which could be used for the purpose of upgrading the CC's security through the use of algorithms that can provide privacy of the large amounts of data.

Another research [8] focuses on a proposal of system integration between IoT and Video Surveillance (VS) technology, with the goal to indulge the requirements of the future needs of VS, and to accomplish a better use of it. The VS data that have been transmitted through the network could be characterized as large-scale data, and thus as BD. The basic outcome of the specific research [8] is an innovative topology paradigm which could offer a better use of IoT technology in VS, and vice-versa.

In [24] initially, it has been presented an analytical study of IoT, CC and BD to resolve various issues that face the health sector in regard to these technologies. In the proposed scenario there is a collection of e-health data by sensor devices and actuators which has been transferred through an established network to a cloud server. These data could be processed in the cloud server in order to be analyzed, and by this analysis there would be born what we call "*data mining*". Moreover, there is a research [24] that deals with security of medical data which constitute sensitive personal data and must be protected.

Moreover, in [3] the authors initially present a survey of the technologies IoT, BD, CC and Monitoring with the aim to discover their common operations and to combine their functionality, in order to achieve beneficial scenarios of their use. The main objective of [3] is to propose a novel system which operates in IoT environment, within there will be collected and managed sensors' data. Additionally, the authors state that their proposed system will be energy efficient and it would be used in a "*Green Smart Building*".

In [12] the authors try to achieve and propose a type of network that will provide more intelligent media-data transfer. Thus, through the study of the use of various open source tools, the authors found the suitable for their experiments tool with the aim to measure the performance of their proposed model of network. At the end, the authors proposed the network topology that they have implemented from a small section of the script of CloudSim simulator with Cooja, so that they could test a single network

segment.

The [25] surveys Social Networking (SNg), BD and CC, focusing on their main features, by concentrating on the security problems of those technologies. In particular, the authors aim to combine the functionality of BD and SNg in CC environment, so that they could analyze the common characteristics and ascertain the advantages of their integration related to security issues. The main outcome of [25] is the presentation of a novel system-framework-network in Cloud environment through which users of various Social Networks (SNs) will be able to exchange data and information, and primarily large-scale data.

To summarize the papers that deal with the Security and Privacy issues of Management in MCC are illustrated [26] [27] [28] [29] [30] [31] [32]. As we can realize there are several works in this field. More particular, in [26] the authors propose an entity-centric approach for an IDM model in Cloud environment. The proposed approach based on two aspects: a) active bundles, and b) anonymous identification. The active bundles include a payload of Personally Identifiable Information, privacy policies and a virtual machine that enforces the policies and additionally the active bundles use a set of protection mechanisms in order to protect themselves. As regard the anonymous identification, they use it with the aim to mediate interactions between the entity and the Cloud services using entity's privacy policies. Moreover, the authors present the main characteristics of the approach which are: a) independent of third party, b) provides minimum information to the Service Provider, and c) provides ability to use identity data on untrusted hosts. Then, the [27] demonstrates the implementation of a mobile system that enables electronic healthcare data storage, update and retrieval using Cloud Computing. The proposed mobile application based in Google's Android OS and offers management of patient health records and medical images. This system was evaluated with the use of Amazon's S3 cloud service. Finally, the authors summarize the details of the implementation and then present initial results of the system in practice. Moreover, the authors of [28] survey the MCC technology, which could help the general readers to have an overview of the MCC including the definition, the architecture, and the applications. Also, the [28] presents the issues, the existing solutions, and the recent approaches of the MCC technology. At the end, the authors discuss a number of future research directions of the MCC. Through the [29] the authors propose a multi-faceted Trust Management system architecture for a cloud computing marketplace, with the aim to support the customers in reliably identifying trustworthy cloud providers. The proposed system offers means to identify the trustworthy cloud providers in term of different attributes that assessed by multiple sources and roots of trust information. Furthermore, the [30] presents a sort survey of MCC evolution and additionally explains how Cloud Computing and Mobile Devices could be combined with good terms for future opportunities, implications and legal issues for developing countries. In another research, the authors of [31] try to review the existing Distributed Application Processing Frameworks, also known as DAPFs, for SMDs in MCC domain. The main objective of [31] is to highlight issues and challenges to existing DAPFs in developing, implementing, and executing computational intensive mobile applications within MCC domain. Thus, through this work the authors propose a thematic taxonomy of the current DAPFs, and then they review current offloading frameworks by using thematic taxonomy, and analyze the implications and critical aspects of current offloading frameworks. Finally, the [31] puts forward open research issues in distributed application processing for MCC that remains to be addressed. Also, the [32] proposes a trust management approach by making an analysis of user behavioral patterns for a reliable Mobile Cloud Computing. So, the authors suggest a method in order to quantify a one-dimensional trusting relation count on the analysis of telephone call data from Mobile Cloud Environment. Subsequently, it is enhanced trustworthiness of data production, management, and overall application.

Finally, in [33] there is a proposal of an efficient algorithm for advanced scalable Media-based Smart Big Data, such as 3D and Ultra HEVC, on Intelligent CC systems. The proposed encoding algorithm of [33] exceeds the conventional HEVC standard which has been demonstrated by the performance evaluations.

Also, related works of other research groups have been studied. The [34] presents a survey on the BD and CC, with the importance to promote the research and

development activities in the sector of the BD and the cloud computing. At the end, the [34] introduces a method for storing the data on cloud using the CloudSim simulation software.

Then, [35] shows an analysis that focuses on the two key concepts, BD and CC, and some of the issues and possibilities which are innate with the deployment of CC and BD services. Through this study is shown which security challenges is among the most prominent problem in CC and BD services. Finally, after there is a consideration about some of the problems related to BD and CC, a number of solutions that have been suggested in [35] towards improving the two key concepts that will go a long way in increasing the adoption rate of CC by organizations.

In [36] the authors surveys on the effects of data processing and analyzing big healthcare data on a CC environment. The [36] proposes the use of the Hadoop, which is a system that could process large amounts of data sets on distributed environments, and also it can be deployed on a CC environment to process the big healthcare data.

The authors in [37] propose an IoT-based security system on smart building scenarios. By this, they are integrating coherent data as fundamental components. The aim of the integration is to drive the building management and security behavior of indoor services accordingly. A holistic platform named City Explorer, which offers security and discovery, is the component in which the proposed system is manifested.

In [38] is illustrated an energy saving solution in buildings aiming to generate predictive models of energy consumption in buildings. Moreover, the authors in [38] use a building as a reference, for which they have one year's unified data, in order to verify the proposed solution. At the end, the authors proposed strategies and control actions for energy saving in the building.

With the aim to take measurements about the temperature, the humidity, and the light in a building, the authors in [39] present an IoT-based sensing and monitoring system which is wirelessly connected. Also, in [39] there is a development of an Android application through which data is transmitted from the LabVIEW, to a "smart" mobile device through which data are monitored remotely.

In [40] the authors analyze the problem of imperfection in smart city data. Additionally, the authors point on the management of these types of data and also create an evidential database with the use of the evidence theory, with the aim to improve the efficiency of the smart city. Moreover, in this paper has been presented a special case of modeling imperfect data in the healthcare sector. Finally, a database which embraces both imperfect and perfect data was built up and the different imperfect aspects, in this database had been represented by the theory of beliefs and illustrated in this paper.

As an attractive service, has been characterized the data sharing service in [41]. As this paper informs us, the attribute based encryption (ABE) is widely discussed, and is the scheme on which the proposed scheme in this paper is based on. This scheme provides solutions for the resource constrained IoT-mobile devices in the clouds. The feasibility and efficiency of the scheme has been proved through performance analysis and experiments which confirm that the scheme is also protected of adaptively chosen ciphertext attacks.

The widely and continuous deployment and use of novel technologies usually leads to threats that come from internal and external factors. A research [42] which deals with the personal mobile data privacy of mobile users provides a protection scheme that is based on the "*Attribute-Based Access Control*" (ABAC) and the data self-deterministic schemes. The "*Attribute-based Semantic Access Control*" (A-SAC) algorithm and the "Proactive Determinative Access" (PDA) algorithm have been used by the authors in [42] to support the proposed sceme. The benefits of the scheme are the constraining data accesses, the proactive prevention of the users' data threats on the cloud, and the increased level of secure sustainability.

Another region based approach that deals with the data safety and the security mechanisms, in the healthcare sector this time, has been presented in [43]. The authors of this paper, through the blend of the RSA (Rivest-Shamir-Adleman) and the AES (Advanced Encryption Standard) algorithms, have been deployed a novel hybrid encryption scheme. The proposed scheme can protect the patients' personal information by concealment of them into a cover image. This image is characterized by high indistinctness, high capacity, and minimized distortion. The feasibility of the scheme is

proved through the comparative analysis that was made between other state-of-the-art methods and the proposed one.

Moreover, the authors of [44] review the current research challenges and opportunities related to the development of secure and safe Intelligent Transport Systems (ITS) applications. Initially, they explore thearchitecture and main features of the ITS systems and also they survey the key enabling standards and projects. Likewise, the authors provide an analysis of a detailed ITS safety application case study and then evaluate in light of the European ETSI TC ITS standard.

Eventually, the [45] states that the Internet of Things could enable innovations that enhance the quality of life, nevertheless IoT generates unprecedented amounts of data that are difficult for traditional systems, Cloud Computing, and even the Edge Computing to handle. Consiquently, Fog Computing is designed to overcome these limitations.

3 Big Data Security Issues

New challenges and standards developed and created in data security issues through the development and the use of BD technology. This creates a growing need for further research on security technologies in order to be able to handhold the large amount of data and to ensure effective. Technologies for securing data are slow when applied to huge amounts of data [3] [12] [21] [33].

TABLE 1
ENCRYPTION RATES OF POPULAR ALGORITHMS

Algorithm	*3-DES*	*AES*	*RSA*
Key length	56, 112 or 168 bits	128, 192 or 256 bits	1024-4096 bits
Megabytes processed	128	256	300
Block size	64 bits	128 bits	512 bits
Rounds	48	10, 12, or 14	1
Time Taken	6,159	4,196	1175,7826
MB per Second	20,783	61,010	10,900

Regarding the Table 1 we can conclude that even the most efficient algorithms give an encryption rate of 64.3MB/s. So, in the sector of BD technology, in which the need of large amounts of data need to be transferred we can see a significant bottle neck for encryption such large amounts data. This is detrimental to the nature of BD which has real time processing and results.

3.1 Big Data on Cloud System Scenario

Among all types of data in the cloud storage, large-scale data has occupied a significant part due to the explosive sharing on social networks and additionally video-on-demand services for movies, TV programs, etc. Moreover, to support users with various bandwidth requirements and device resolutions and full interactive playback in large-scale data demand, usually various versions at different bitrates are generated [3] [12] [21] [33] [46] [47] [48].

Schemes for large-scale data, named as Big Data, have shown good performances in cloud storage under different configurations. However, these codes treat all files as general data, in which one unrecoverable error will lead to permanent loss of the whole file. They do not consider the features of specific data types.

In this work, we propose Cloud-based system for BD used and transmitted through an IoT network.

4 Internet of Things

The IoT could be characterized as "*a network of devices that transmits, shares, and uses data from the physical environment to provide services to individuals, corporations, and society*" [1] [8] [12], which already defined in the Introduction Section. Also, IoT has multiple applications in health, transport, environment, energy or types of devices such as sensors, devices worn/carried (wearable), watch, glasses, home automation (domotics).

4.1 Advantages of the data

Chances where the streaming data will produce novel markets with the aim to inspire positive change or to intensify existing services are examined by businesses. Some examples of fields that are at the heart of these developments are listed below [49]:

a) ***IoT(a)***: Smart solution in the bucket of transport: With this could achieve better solutions in transportation sector with the aim to provide a better way of living.
b) ***IoT(b)***: Smart power grids incorporating more renewable: With this the system reliability could be achieved and also it could be reduced the charges consumers, thus providing cheaper electricity.
c) ***IoT(c)***: Remote monitoring of patients: With this we could achieve a system which offers remote monitoring of patients. This system could offer a better and well-managed healthcare system by improving the quality of services, increasing the number of people served, and saving money.
d) ***IoT(d)***: Sensors in homes and airports: With this we could achieve safer places such as airports and houses, by establishing a number of sensors in the field.
e) ***IoT(e)***: Engine monitoring sensors that detect & predict maintenance issues: With this we detect and predict maintenance issues, improve inventory replenishment, and even define priorities in scheduling maintenance work, repairs, and regional operations.

4.2 Security

The security of IoT systems is a field of strives concerned with safeguarding connected devices and networks in the IoT. The IoT involves the growing pervasiveness of objects and the entities provided with unique identifiers and the ability to automatically transmit data through a network. The major impact of the increased use of IoT communication came from computing devices and embedded sensor systems which used in industrial machine-to-machine (M2M) communication, and technologies such as smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices [2] [22] [50] [51].

The huge issue is that security has not always been considered in product design due to the idea of networking appliances and other objects were relatively new. Aiming to improve security and privacy issues, an IoT device that needs to be directly accessible through the Internet should be portioned into its own network and has limited network access. The network portion should be monitored in order to identify the potential abnormal traffic, and if there is any problem, action should be taken [2] [22] [50] [51] [52].

In the sector of IoT technology there are System models. A wireless network model with a source-destination pair, N trusted relays and J eavesdroppers $(J \leq 1)$ are considered. Suppose that the global CSE is available. The eavesdropper channel, source encoding schemes, decoding models and accommodative protocol are admitted to be public, only source message is assumed to be confidential. In this work, the discussion is limited to two main accommodative models: Decode-and-Forward (DF) and Amplify-and-Forward (AF) [52] [53] [54].

Decode-and-forward (DF)

Two are the main stages in DF model. In Stage 1, the source broadcasts its encoded

symbols to its trusted relays using the first transmission slot. When the symbol x transmitted, the received signals at the N relays are given by (1),

$$y_r = \sqrt{P_s} h_{SR}^* x + n_r \quad (1)$$

where Ps is the transmit power of source and nr is the noise vector at relays [53].

In Stage 2, all the trusted relays that successfully decode the message, re-encode the message and accommodative transmit the re-encoded symbols to the destination by using the second transmission slot. Each relay transmits a weighted version of the re-encoded symbol. When transmitting the symbol $\tilde{x}$, the received signal at the destination is given by (2),

$$y_d = h_{RD}^\dagger w \tilde{x} + n_d \quad (2)$$

while the received signal at the listeners is expressed in vector form as (3),

$$y_e = H_{RE}^\dagger w \tilde{x} + n_e \quad (3)$$

The transmit power budget for Stage 2 is considered to be P - P_s where P is the total power for transmitting one symbol and P_s is the transmit power of source [53].

Amplify-and-forward (AF)

At the other hand, the AF model is additionally a two-stage model such as the DF model. The Stage 1 is similar for both AF and DF models, except that the transmit power can be different. The trusted relays forward the signals that are received during Stage 1 to the destination, using the second transmission slot in Stage 2. That is, each relay transmits a weighted version of the noisy signal that they received during Stage 1. The transmitted signals of all relays are denoted by the product of $diag\{w\}y_r$, where w is the weight vector and yr is given by (1). The received signal at the destination is given by [53],

$$y_d = \sqrt{P_s} h_{RD}^\dagger diag\{w\} h_{SR}^* x + h_{RD}^\dagger diag\{w\} n_r + n_d \quad (4)$$

The received signals at the listeners, in a vector form, is denoted by [49],

$$y_e = \sqrt{P_s} H_{RE}^\dagger diag\{w\} h_{SR}^* x + H_{RE}^\dagger diag\{w\} n_r + n_e \quad (5)$$

Also, another security challenge in IoT is the encryptions algorithm. The RSA algorithm, which is the most commonly used public key algorithm in the Internet, and it can be used in sensor networks by establishing a Trusted Platform Module (TPM), which costs less than 5% of a common sensor node [54]. So, the memory has been measured for a fully authenticated handshake with 2048-bit RSA keys. This type of handshake has the largest memory requirements since it needs more code and buffer space for the client's Certificate and Certificate-Verify messages. The memory increased its use because the code basically contains hundreds of statements form buffer[x] = 0xff. The use of this encryption algorithm in IoT's security could offer better communication privacy in its functionality.

5 Cloud Computing

CC offers abilities and functions such as computing, storage, services, and applications over the Internet. In general, to render smartphones energy efficient and computationally capable, major changes to the hardware and software level are required. This causes the cooperation of developers and manufacturers [55].

5.1 Features

As all technologies, so the CC technology has a number of characteristics which determine its operation. These characteristics are represented and outlined below.

CC(a): *Storage over Internet*

Storage over Internet can be defined as "*a technology framework that uses Transmission Control Protocol/Internet Protocol (TCP/IP) networks to link servers and storage devices and to facilitate storage solution deployment*" [56] [57].

CC(b): *Service over Internet*

The Service over Internet has as major objective is to "*help customers all over the world in order to transform aspirations into achievements by harnessing the Internet's efficiency, speed and ubiquity*" [56] [57].

CC(c): *Applications over Internet*

Cloud Applications, or as scientific known as Applications over Internet, are the programs which have been written to do the job of a current manual task, or virtually anything, and which perform their job on the server through an internet connection [56] [57].

CC(d): *Energy Efficiency*

Energy Efficiency could be defined as *"a way of managing and restraining the growth in energy consumption*" [56] [57]. By delivering more services for the same energy input or for the same services for less energy input may be something more energy efficient [56] [57].

CC(e): *Computationally Capable*

The services of computational clouds are leveraging the computationally concentrated and ubiquitous mobile applications which have been enabled by the technology of MCC. Thus, a system can be considered as computationally capable when it meets the requirements to offer us the results we want, by making the right calculations [56] [57].

5.2 Security on Cloud Computing

CC security is an evolving sub-domain of computer security, network security and information security. It makes an allusion to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of CC.

CC technology offers through its storage solutions to users and industries various capabilities with the aim to store and process their data in third-party data centers [58]. Thus, by aiming to offer secure communication through the network, encryption algorithm plays a vital role. As regards the researches that have been made, an important encryption technique is the Symmetric Key Encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. In this encryption technique the most used algorithm is the AES [59] [60].

AES (Advanced Encryption Standard) is the newest encryption standard and the more reliable, recommended by NIST to replace DES algorithm. The only effective scenario of attacking in AES is the Brute force attack, in which the attacker tries to test all the characters combinations to unlock the encryption. AES encryption model is fast and flexible, and in addition, it can be implemented on different platforms [61]. Bellow, a sample-part of the AES encryption algorithm is represented.

Algorithm: sample of AES

```
Cipher(byte[] input, byte[] output)
{
    byte[4,4] State;
    copy input[] into State[] AddRoundKey
    for (round = 1; round < Nr-1; ++round)
    {
        SubBytes  ShiftRows  MixColumns
AddRoundKey
    }
    SubBytes ShiftRows AddRoundKey
    copy State[] to output[]
}
```

AES algorithm characterized as better and safer than other algorithms for a number of reasons, which is follows [62]:

- It performs consistently well in both hardware and software platforms under a wide range of environments. These include 8-bit and 64-bit platforms and DSP's.
- Its inherent parallelism facilitates efficient use of processor resources resulting in very good software performance.
- This algorithm has speedy key setup time and good key agility.
- It requires less memory for implementation, making it suitable for limited-space environments.
- The structure has good potential for benefiting from instruction-level parallelism.
- There are no serious weak keys in AES.
- It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits).
- Statistical analysis of the cipher text has not been possible even after using huge number of test cases.
- No differential and linear cryptanalysis attacks have been yet proved on AES.

5.3 Cloud Computing trade offs

Cloud Computing has some disadvantages-limitations which should be eliminated over the years in order to achieve a better and more ideal use. Some businesses and especially the smaller ones need to be aware of these limitations before going in for this technology.

CC(l-a): *Security*

One major issue of the Mobile Cloud Computing is the security issue. Before someone adopts this technology, they should know that all the company's sensitive information would be surrender to a third-party Cloud service provider. This could potentially put the company in great risk. Hence, someone must be absolutely sure that they would choose the most reliable service provider, who will keep the information completely safe [11] [36] [64].

CC(l-b): *Connectivity*

Internet connection is critical to Cloud Computing. Thus, the user should be certain that there is a good result before opting for these services. Since someone owes a mobile device which is connected to the internet has become the norm in the wireless world of today, Cloud Computing has a very large potential user base [11] [65].

CC(l-c): *Performance*

Another major concern of the Cloud Computing pertains to its performance. Some users feel performance is not as good as in native applications. Thus, checking with one service provider and understanding their track record is advisable [11] [66] [67].

CC(l-d): *Latency (Delay)*

In Cloud Computing, latency (sometimes referred as turnaround time) is defined as the time involved in offloading the computation and getting back the results from the nearby infrastructure or cloud [11] [15].

CC(l-e): *Privacy*

Data privacy is important and is one of the main bottlenecks that restrict consumers from adopting Cloud Computing. Therefore, to gain consumers trust in the Cloud, the application models must support application development with privacy protection, and implicit authentication mechanisms [11] [64] [68].

6 IoT & Cloud Computing Integration

Moreover, a new generation of services, coount on the concept of the "*cloud computing*", has made its appearance in the last few years with the purpose of offering access to services and the data from any place and at any time [69]. CC is a technology that can be set as a base technology in the use of IoT [70].

A number of the major characteristics of the CC technology which relate to the features of IoT are: a) Storage over Internet, b) Service over Internet, c) Applications over internet, d) Energy efficiency and e) Computationally capable. Tables 2 presents the features of CC regarding the accessibility of this technology provides when combined with the characteristics of IoT [69] [70].

TABLE 2
CONTRIBUTIONS OF CLOUD COMPUTING IN INTERNET OF THINGS

Internet of Things characteristics	*CC(a)*	*CC(b)*	*CC(c)*	*CC(d)*	*CC(e)*
IoT(a)	**X**	**X**	**X**		**X**
IoT(b)	**X**	**X**		**X**	**X**
IoT(c)		**X**	**X**		**X**
IoT(d)	**X**	**X**	**X**	**X**	**X**
IoT(e)		**X**	**X**	**X**	**X**

Table 2 represents the characteristics of CC technology regarding the suitableness of this technology provides. Furthermore, it enumerates the major features of the IoT technology. The main objective of Table 2 is to show which of the specific characteristics of CC technology, related more and improve the functionality of the characteristics of IoT technology. As we can observe from Table 2, the characteristic of IoT which affected more by the characteristics of CC is "*Sensors in homes and airports*". Regarding the CC, the feature which affected more are "*Service over Internet*" and "Computationally capable". As a general conclusion, we can observe that those two technologies contribute more each other in many of their features.

6.1 Security issues in IoT and Cloud Computing integration

There is a rapid and self-sufficient evolution taking into account the two technologies of IoT and CC. Initially, the virtually unlimited capabilities and resources of CC with aim to remunerate its technological constrains, such as processing, storage and

communication, could be a beneficial scenario for the IoT technology. In many cases, CC can offer the transitional layer between the things and the applications, hiding all the complexity and functionalities which are necessary to implement the latter [71].

Through the integration of IoT and CC could be observed that CC can fill some gaps of IoT such the limited storage and applications over internet. In the other hand, IoT can also fill some gaps of CC such the major problem of limited scope. Count on motivations such those referred previously and the important issue of security in both technologies we can consider some drivers for the integration. The security issue of this integration has a serious problem. When critical IoT applications move towards the CC technology, concerns arise due to the lack of trust in the service provider or the knowledge about service level agreements (SLAs) and knowledge about the physical location of data. Consequently, new challenges require particular attention as mentioned in surveys [72] [73]. Moreover, public key cryptography could not be applied at all layers due to the computing power constraints imposed by the things [72]. These are examples of topics that are currently under examination in order to tackle the big challenge of security and privacy in CC and IoT integration [71].

Subsequently, some challenges about the security problem in the integration of those technologies are listed below [71].

a) *Heterogeneity*: A big challenge in CC and IoT integration is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications [74].
b) *Performance*: Often CC and IoT integration's applications introduce particular performance and QoS requirements at several levels and in some specific scenarios meeting requirements might not be easily achievable [75].
c) *Reliability*: When CC and IoT integration is adopted for mission-critical applications, reliability concerns typically arise [76].
d) *Big Data*: With an estimated number of 50 billion devices that will be networked by 2020, particular attention must be paid to transportation, storage, access, and processing of the large amount of data they will produce [77].
e) *Monitoring*: This is an essential activity in CC environments for capacity planning, for managing resources, SLAs, performance and security, and for troubleshooting [78].

TABLE 3
AFFECTS OF IOT & CLOUD COMPUTING SECURITY CHALLENGES

IoT & Cloud Computing security challenges	*Internet of Things*	*Cloud Computing*
Heterogeneity		**X**
Performance	**X**	**X**
Reliability	**X**	
Big Data	**X**	**X**
Monitoring	**X**	

Table 3 shows the two technologies that we survey in this work and the challenges of their integration that arising from our study. These challenges are related to the security problem in the integration of two aforementioned technologies and they listed in detailed in subsection 6.1 (A Security issues in IoT and Cloud Computing integration). As we can observe from Table 3, the both technologies have two common main challenges of their integration which are Performance and Big Data. Additionally,

we can observe that IoT technology is related to more challenges (4) than the CC technology (3).

6.2 Big Data based on Cloud Server

In order to combine BD technology with CC technology and to achieve a beneficial operation of BD in Cloud environment we have to study the relation of their basic features [3] [12] [22] [51].

Initially, we have to define which are the basic features of BD, which are widely known as the 5 Vs of Big Data. In particular the 5 Vs of BD are: 1)*Volume*: the vast amounts of data created every second, 2)*Velocity*: the speed at which new data is created and the speed at which data moves around, 3)*Variety*: the different types of data we can now use. In the past we focused on structured data that neatly fits into tables or relational databases, such as financial data, 4)*Veracity*: the messiness or trustworthiness of the data, 5)*Value*: all well and good having access to big data but unless we can turn it into value it is useless [22] [51].

TABLE 4
CORRELATION OF BD AND CC CHARACTERISTICS

Big Data Features / *Cloud Computing Features*	***Volume***	***Velocity***	***Variety***	***Veracity***	***Value***
Storage over Internet		**X**		**X**	**X**
Service over Internet	**X**		**X**	**X**	**X**
Applications over Internet	**X**	**X**	**X**	**X**	**X**
Energy Efficiency	**X**	**X**			
Computational Capable		**X**	**X**		**X**

Table 4 demonstrates the basic features of BD (5 Vs) and how they are contributed by the major features of CC. As we can observe, there are two the key features of BD technology which contributes more with the characteristics of CC technology are *Velocity* and *Value*. *Velocity* and *Value* contribute four from the five key features of CC. Also, another thing that we can observe from Table 4 is that the feature *Applications over Internet* contributed from all the key features of BD.

6.3 Proposed Efficient IoT and Cloud Computing Security Model

As we can infer, by taking advantage of the reasons which AES algorithm offers better secure in CC and the two models that give benefits in security problems in IoT we can propose a novel method that uses those benefits with the aim to improve the security and privacy problems in the integration of two technologies.

The AES algorithm offers the ability to have speed key setup time a good key agility. So, if we use this algorithm in the functionality of DF model, we could have a trusted relay method with an encryption of a speed key setup. Therefore, instead the trust relay use that DF and AF methods offer we can seize additionally there no serious weak keys in AES and so we could have a beneficial security use of the encryption in the integrated new model. Moreover, we can take advantage the less memory which AES needs for implementation that makes it for restricted-space environments. So, we can seize the transmit power that the AF model offers and as a result we can have a better and more trusted transmission. In the way of transmission, when the symbol transmitted with the use of DF model, the received signal at destination is given by the equation (2),

which mentioned in previous section.

With this proposed model we can extend the advances of IoT and CC, by developing a highly innovative and scalable service platform to enable secure and privacy services. Through this research we can propose the following part of algorithm which extends the security advances of both technologies. As a proposal of this work could be this part of pseudocode algorithm which uses the original key consists of 128 bits/16 bytes which are represented as a 6x6 matrix, represented bellow.

Algorithm 1: pseudocode

```
input -> byte[]
byte[] + R.Key -> state[]
for 6 to 66
  W[i-1] -> T
  if i mod 6 = 0
                rotate T + 6
      W[i-6] / T -> W[i]
      R.Key+1
      i+1 -> i
Row +1 -> Row
state[] -> output[]
```

Algorithm 1 represents the procedure implementing in the server aiming to achieve better results of securing the data transmitted. Moreover, this procedure could be achieved in a limited number of loops of the algorithm. The algorithm takes as input data the transmitted signal and then with the use of AES algorithm and the key generated tries to decrypt the data by using the original key consists of 128 bits/16 bytes which are represented as a 6x6 matrix. Through tis procedure we could achieve the less of loops of the algorithm and in addition to this we can achieve a more secure data decryption/encryption system for transmitting the data through the network.

6.4 Experimental Results

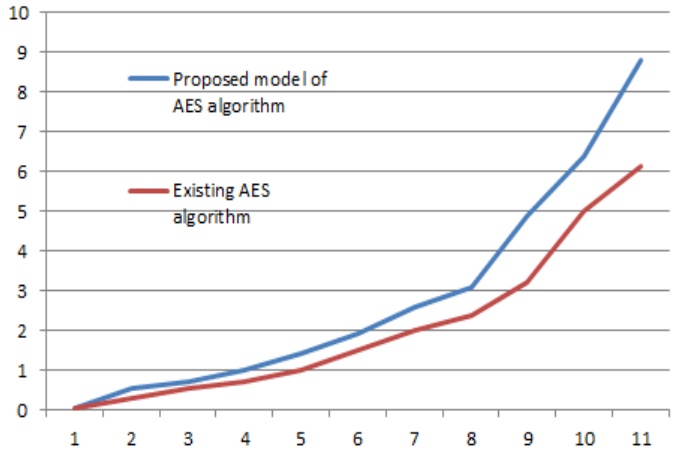


Fig. 1. Security level of encryption algorithms of measurement used for the study of AES model algorithm.

Considering the benefits of the security models and algorithms of IoT and CC technologies we can observe that we can have a beneficial use of integration those two technologies. Instead of the wide use of IoT we can take advantage that CC security

through the AES algorithm performs consistently well in both hardware and software platforms under a wide range of environments. This use could be possible for all type of platforms and DSPs. Furthermore, the novel integrated technology could has good potential for benefiting from instruction-level parallelism and will support any type of block sizes and key sizes that are multiples of 32 and used both of IoT and CC. Also, each transmitted signal through the new technology can transmitted as a relay and trusted signal with a weighted version of the re-encoded symbol.

Through this integration we can achieve some useful functions, i.e. we can use the Cloud-based IoT service with the aim to connect sensors and additionally made them capable to share the sensor readings with others, reducing the security issues. Furthermore, another useful operation is that we can use the HTTP protocol with the aim to send data between IoT things and the CC applications. Moreover, some of the key advantages and challenges that can be defined from this integration are: 1) Both the physical hardware manufacturing resource and software manufacturing can be intelligently perceived and connected into the wider networks with the support of IoT technologies. 2) The collected information and data can be communicated and transmitted between M2M under the support of specific IoT technologies. 3) The collected and transmitted information can be processed and computed according to particular requirements under the support of different CC service, and some useful data and decision information can be intelligently generated and obtained.

TABLE 5
AES CONTRIBUTION IN IOT AND CLOUD COMPUTING

AES Characteristics	*Internet of Things*	*Cloud Computing*	*IoT & CC integration*
Key length	**X**	**X**	**X**
Rounds		**X**	**X**
Certifications	**X**	**X**	**X**
Speed	**X**		**X**

The Tables 5 exhibiting the key features of the two encryption algorithm that used with the aim to achieve integration of the technologies of IoT and CC concerning the security problem. Table 5 presents which of the key features of AES encryption algorithm contributes both IoT and CC technologies, and at the end how completely contributes the integration model of IoT and CC.

Figure 1 shows, the measurements that have been through time. As we can observe by this figure the more often is the combined use of the algorithms, the higher level of security of the data usage we get every time. The upper line represents our proposed model of AES algorithm and the other (down line) represents the existing AES algorithm.

TABLE 6
CORRELATION OF BD CHARACTERISTICS WITH IOT & CC INTEGRATION MODEL

Big Data Features	***Volume***	***Velocity***	***Variety***	***Veracity***	***Value***
IoT & CC integration model	**X**	**X**	**X**	**X**	**X**

The Tables 6 exhibits the key features of BD and which of those characteristics could be contributed by the integration method of the technologies IoT and CC concerning the security problem. Table 6 presents that all the characteristics of BD contributed by the integration model of IoT and CC technologies.

7 Conclusions

The CC technology provides a number of possibilities, but additionaly places several limitations as well. Cloud Computing refers to an infrastructure where both the data storage and the data processing happen outside of the mobile device. Also, the IoT is a new technology which is growing rapidly in the field of telecommunications, and especially in the modern sector of wireless telecommunications.

The main objective of the interaction and cooperation between things and objects sent through the wireless networks is to fulfil the objective set to them as a combined entity, with the aim to achieve a better environment for the use of Big Data. In addition, based on the technology of wireless networks, both the technologies of CC and IoT develop rapidly. In this work, we present a survey of IoT and CC with a focus on the security problems of both technologies. Particularly, we combine the two aforementioned technologies with the aim to examine the familiar characteristics, and with the aim to discover the benefits of their integration in order to secure the use and the transmission of Big Data. At the end, the security challenges of the integration of IoT and CC were surveyed through the proposed algorithm model, and additionally there is a presentation of how the two encryption algorithms which were used contributes in the integration of IoT and CC as base technologies for Big Data. This and additionally the security challenges that surveyed in this work can be the domain of future research on the integration of those two technologies.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and feedback which was extremely helpful in improving the quality of the paper.

References

[1] L. Atzori et al, "The Internet of Things: A survey", Computer Networks, no. 54, p. 2787–2805, 28/10/2010.

[2] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, December 2016.

[3] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, B. B. Gupta, “Efficient IoT-based sensor BIG Data collection-processing and analysis in Smart Buildings”, Future Generation Computer Systems, vol. 82, pp. 349-357, May 2018.

[4] M. Hilbert, P. López, “The World’s Technological Capacity to Store, Communicate, and Compute Information”, Science, vol. 332, issue: 6025, pp. 60–65. 2011.

[5] Z. Fu et al, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, 2015.

[6] J. Mongay Batalla, P. Krawiec, “Conception of ID layer performance at the network level for Internet of Things”, Springer Journal Personal and Ubiquitous Computing, Vol.18, Issue 2, pp. 465-480, 2014.

[7] C. Stergiou, K. E. Psannis, “Efficient and Secure Big Data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017.

[8] C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, “Architecture for Security in IoT Environments”, in Proceedings of 26th IEEE International Symposium on Industrial Electronics, 19-21 June 2017, Edinburgh, Scotland, UK.

[9] A. R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou, “A Roadmap for Security Challenges in Internet of Things”, Elsevier, Digital Communications and Networks (DCN), vol. 4, issue: 2, pp. 18-137, April 2018.

[10] Y. Kryftis, G. Mastorakis, C. Mavromoustakis, J. Mongay Batalla, E. Pallis and G. Kormentzas, "Efficient Entertainment Services Provision over a Novel Network Architecture". To be published in IEEE Wireless Communications Magazine, 2016.

[11] C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley, International Journal of Network Management, pp. 1-12, May 2016.

[12] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B.-G. Kim, "Algorithms for efficient digital media transmission over IoT and cloud networking", Journal of Multimedia Information System, vol. 5, no. 1, pp. 1-10, March 2018.

[13] C. Stergiou, K. E. Psannis, A. P. Plageras, G. Kokkonis, Y. Ishibashi, "Architecture for security monitoring in IoT environments", in Proceedings of IEEE 26th International Symposium on Industrial Electronics, Edinburgh, Scotland, UK, June 2017.

[14] A. P. Plageras, K. E. Psannis, Y. Ishibashi, B.-G. Kim, "IoT-based Surveillance System for Ubiquitous Healthcare," Industrial Electronics Society, in Proceedings of IEEE/IECON 2016 - 42nd Annual Conference of the IEEE, October 2016.

[15] J. Li, L. Huang, Y. Zhou, S. He, Z. Ming ,"Computation partitioning for mobile cloud computing in big data environment", IEEE Transactions on Industrial Informatics, Vol. 11 January 2017.

[16] R. Yu, X. Huang, J. Kang, J. Ding, S. Maharjan, S. Gjessing, Y. Zhang, "Cooperative Resource Management in Cloud-Enabled Vehicular Networks", IEEE Transactions on Industrial Informatics, volume: 62, Issue: 12, pp 7938 - 7951, September 2015.

[17] D. Agrawal, B. B. Gupta, S. Yamaguchi, K. E. Psannis, "Recent Advances in Mobile Cloud Computing", Wireless Communications and Mobile Computing, December 2017.

[18] A. M. M. Ali, N. M. Ahmad, A. H. M. Amin, "Cloudlet-based cyber foraging framework for distributed video surveillance provisioning", Information and Communication Technologies (WICT), 2014 Fourth World Congress on, Bandar Hilir, Malaysia, December 2014.

[19] M. R. Rahimi et al, "Mobile Cloud Computing: A survey, State of Art and Future Directions", Mobile Networks and Applications, Volume 19, Issue 2, pp. 133-143, March 2014.

[20] S. Fremdt, R. Beck, S. Weber, "Does Cloud Computing Matter? An analysis of the Cloud Model software-as-a-service and its impact on operational agility" 46th Hawaii International Conference on System Sciences, pp. 1025-1034, October 2013.

[21] C. Stergiou, K. E. Psannis, "Algorithms for Big Data in Advanced Communication Systems and Cloud Computing", in Proceedings of 19th IEEE Conference on Business Informatics 2017 (CBI2017), Doctoral Consortium, 24-26 July 2017, Thessaloniki, Greece.

[22] A. P. Plageras, C. Stergiou, K. E. Psannis, Byung-Gyu Kim, Brij Gupta, Y. Ishibashi, "Solutions for Inter-connectivity and Security in a Smart Hospital Building", in Proceedings of 15th IEEE International Conference on Industrial Informatics (INDIN 2017), 24-26 July 2017, Emden, Germany.

[23] C. Thirumalai, H. Kar, "Memory Efficient Multi Key (MEMK) Generation Scheme for Secure Transportation of Sensitive Data over Cloud and IoT Devices", IEEE, in Proceedings of 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), 21-22 April 2018, Vellore, india.

[24] A. P. Plageras, C. Stergiou, K. E. Psannis, G. Kokkonis, Y. Ishibashi, Byung-Gyu Kim, Brij Gupta, "Efficient Large-Scale Medical Data (eHealth Big Data) Analytics in Internet of Things", in Proceedings of 19th IEEE International Conference on Business Informatics

(CBI'17), International Workshop on the Internet of Things and Smart Services (ITSS2017), 24-26 July 2017, Thessaloniki, Greece.

[25] C. Stergiou, K. E. Psannis, A. P. Plageras, T. Xifilidis, B. B. Gupta, "Security and Privacy of Big Data for Social Networking Services in Cloud", in Proceedings of IEEE conference on Computer Communications (IEEE INFOCOM 2018), 15-20 April 2018, Honolulu, HI, USA.

[26] P. Angin, B. Bhargava, R. Ranchal, N. Singh, M. Linderman, "An Entity-centric Approach for Privacy and Identity Management in Cloud Computing", in Proceedings of 29th IEEE International Symposium on Reliable Distributed Systems, 31 October-3 November 2010, New Delhi, India. [DOI: 10.1109/SRDS.2010.28]

[27] C. Doukas, T. Pliakas, I. Maglogiannis, "Mobile Healthcare Information Management utilizing Cloud Computing and Android OS", in Proceedings of 32nd Annual International Conference of the IEEE EMBS 2010, 31 August-4 September 2010, Buenos Aires, Argentina.

[28] H. T. Dinh, C. Lee, D. Niyato, P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", Wireless Communications and Mobile Computing, vol. 13, pp. 1587-1611, October 2011. [DOI: 10.1002/wcm.1203]

[29] S. M. Habib, S. Ries, M. Muhlhauser, "Towards a Trust Management System for Cloud Computing", in Proceedings of IEEE International Joint Conference TrustCom-11/IEEE ICESS-11/FCST-11, 16-18 November 2011, Changsha, China.

[30] M. R. Prasad, J. Gyani, P.R. K. Murti, "Mobile Cloud Computing: Implications and Challenges", Journal of Information Engineering and Applications, vol. 2, no. 7, pp. 7-15, October 2012.

[31] M. Shiraz, A. Gani, R. H. Khokhar, R. Buyya, "A Review on Distributed Application Processing Frameworks in Smart Mobile Devices for Mobile Cloud Computing", IEEE Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1294-1313, November 2012.

[32] M. Kim, S. O. Park, "Trust management on user behavioral patterns for a mobile cloud computing", Springer, Cluster Computing, vol. 16, issue 4, pp. 725-731, December 2013. [DOI: 10.1007/s10586-013-0248-9]

[33] C. Stergiou, K. E. Psannis, B. B. Gupta, "Advanced Media-based Smart Big Data on Intelligent Cloud Systems", IEEE Transaction on Sustainable Computing, in Press , 2018.

[34] A. A. Gnana Singh et al, "A Survey on Big Data and Cloud Computing", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 7, no. 4, pp. 273-277, July 2016.

[35] O. Awodele et al, "Big Data and Cloud Computing Issues," International Journal of Computer Applications, vol. 12, no. 133, pp. 14-19, January 2016.

[36] S. Rallapallia et al, "Impact of Processing and Analyzing Healthcare Big Data on Cloud Computing Environment by Implementing Hadoop Cluster," International Conference on Computational Modeling and Security (CMS2016), pp. 16-22, December 2015.

[37] J. L. Hernandez-Ramos, M. V. Moreno, J. B. Bernabe, D. G. Carrillo, A. F. Skarmeta, "SAFIR: Secure access framework for IoT-enabled services on smart buildings", Journal of Computer and System Sciences, vol. 81, issue: 8, pp. 1452-1463, December 2015.

[38] M. V. Moreno, L. Dufour, A. F. Skarmeta, A. J. Jara, D. Genoud, B. Ladevie, J.-J. Bezian, "Big data: the key to energy efficiency in smart buildings", Soft Computing, vol. 20, issue: 5, pp. 1749-1762, May 2016.

[39] J. Shah, B. Mishra, "Customized IoT Enabled Wireless Sensing and Monitoring Platform for Smart Buildings", Procedia Technology, vol. 23, pp. 256-263, February 2016.

[40] Hatem Ben Sta, "Quality and the efficiency of data in "Smart-Cities"", Future Generation Computer Systems, vol. 74, pp. 409-416, 2017.

[41] J. Li, Y. Zhang, X. Chen, Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing", Elsevier, Computers & Security, vol. 72, pp. 1-12, January 2018.

[42] M. Qiu, K. Gai, B. Thuraisingham, L. Tao, H. Zhao, "Proactive user-centric secure data scheme using attribute-based semantic access controls for mobile clouds in financial industry", Elsevier, Future Generation Computer Systems, vol. 80, pp. 421-429, March 2018.

[43] M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, Arunkumar N, A. Farouk, "Secure Medical Data Transmission Model for IoT-Based Healthcare Systems", IEEE Access, vol. 6, pp. 20596 – 20608, March 2018.

[44] E. B. Hamida, H. Noura, W. Znaidi, "Security of Cooperative Intelligent Transport Systems: Standards, Threats Analysis and Cryptographic Countermeasures", Electronics, vol. 4, issue: 3, pp. 380-423, July 2015.

[45] A. V. Dastjerdi, R. Buyya, "Fog Computing: Helping the Internet of Things Realize Its Potential", IEEE, Computer, vol. 49, issue: 8, August 2016.

[46] K. Müller et al, "3D High-Efficiency Video Coding for Multi-View Video and Depth Data", IEEE Transactions on Image Processing, vol. 9, no. 22, pp. 3366-3378, September 2013.

[47] L. Shen et al, "An Effective CU Size Decision Method for HEVC Encoders", IEEE Transactions on Multimedia, vol. 2, no. 15, pp. 465-470, February 2013.

[48] Jens-Rainer Ohm et al, "Comparison of the Coding Efficiency of Video Coding Standards-Including High Efficiency Video Coding (HEVC)", IEEE Transactions on Circuits and Systems for Video Technology, vol. 12, no. 22, pp. 1669-1684, December 2012.

[49] J. M. Batalla, "Advanced multimedia service provisioning based on efficient interoperability of adaptive streaming protocol and high efficient video coding," Journal of Real-Time Image Processing, pp. 1-12, March2015.

[50] M. Rouse, "IoT security (Internet of Things security)," IoT Agenda, 01/11/2015. [Online]. Available: http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security. [Accessed 27/07/2016].

[51] A. P. Plageras, K. E. Psannis, "Algorithms for Big Data Delivery over the Internet of Things", in Proceedings of 19th IEEE Conference on Business Informatics 2017 (CBI2017), Doctoral Consortium, 24-26 July 2017, Thessaloniki, Greece.

[52] L. Dong, Z. Han, A. P. Petropulu, H. V. Poor, "Improving Wireless Physical Layer Security via Cooperating Relays", IEEE Transactions on Signal Processing, VOL. 58, No. 3, March 2010.

[53] A. K. Nair et al, "Analysis of Physical layer Security via Co-operative Communication in Internet of Things," International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST - 2015), no. 24, p. 896 – 903, January 2016.

[54] W. Hu, H. Tan, P. Corke, W. C. Shih, S. Jha, "Toward trusted wireless sensor networks", ACM Transactions on Sensor Networks, vol. 7, issue 5, pp. 1-25, 2010.

[55] D. Huang, "Mobile cloud computing," IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, vol. 6, no. 10, pp. 27–31, 2011.

[56] G. Md Whaiduzzaman et al, "A Study on Strategic Provision of Cloud Computing Services", The Scientific World Journal, pp. 1-8, June 2014.

[57] S. K. Garg, S. Versteeg, R. Buyya, "A framework for ranking of cloud computing services", Future Generation Computer Systems, vol. 29, issue: 4, pp. 1012–1023, 2013.

[58] Mohammad Haghighat et al, "CloudID: Trustworthy cloud-based and cross-enterprise biometric identification," Expert Systems with Applications, vol. 11, no. 42, pp. 7905-7916, November 2015.

[59] Y. Kumar, R. Munjal, H.Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, October 2011.

[60] R. Kaur, S. Kinger, "Analysis of Security Algorithms in Cloud Computing," International Journal of Application or Innovation in Engineering & Management (IJAIEM), vol. 3, no. 3, pp. 171-176, March 2014.

[61] G. Singh, S. Kinger, "Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July 2013.

[62] A. Sachdev, M. Bhansali, "Enhancing Cloud Computing Security using AES Algorithm," International Journal of Computer Applications, vol. 9, no. 67, pp. 19-23, April 2013.

[63] P. Viswanathan, "Cloud Computing – Is it Really All That Beneficial?", abouttech, 7/7/2012. [Online]. Available: http://mobiledevices.about.com/od/additionalresources/a/Cloud-Computing-Is-It-Really-All-That-Beneficial.htm. [Accessed 24/5/2017].

[64] F. Pfarr, T. Buckel, A. Winkelmann, "Cloud Computing Data Protection – A Literature Review and Analysis", in Proceedings of 47th Hawaii International Conference on System Sciences, pp. 5018-5027, 6-9 January 2014, Waikoloa, HI, USA.

[65] E. Almrot, S. Andersson, "A study of the advantages & disadvantages of mobile cloud computing versus native environment", Digitala Vetenskapliga Arkivet, Bachelor Thesis in Software Engineering, Blekinge Institute of Technology, Karlskrona, May 2013.

[66] S. Fremdt, R. Beck, S. Weber, "Does Cloud Computing Matter? An analysis of the Cloud Model software-as-a-service and its impact on operational agility", in Proceedings of 46th Hawaii International Conference on System Sciences 2013, pp. 1025-1034, 7-10 January 2013, Waileam Maui, Hi, USA.

[67] Blog: Follow what's happening at Get Cloud Services, "Mobile Cloud Computing – Pros and Cons," GetCloud Services, 23/12/2014. [Online]. Available: https://www.getcloudservices.com/blog/mobile-cloud-computing-pros-and-cons/. [Accessed 24/12/2017].

[68] E. Shi, Y. Niu, M. Jakobsoon, R. Chow, "Implicit Authentication through Learning User Behavior", ACM, in Proceedings of ISC'10 13th International Conference on Information Security, pp. 99-113, 25-28 October 2010, Boca Raton, FL, USA.

[69] The NIST definition of cloud computing, National Institute of Standards and Technology. [Accessed 24/07/2015].

[70] Huang D. Mobile Cloud Computing. IEEE COMSOC Multimedia Communications Technical Committee (MMTC) E-Letter, vol. 6, issue: 10, pp. 27–31, 2011.

[71] A. Botta et al, "Integration of Cloud Computing and Internet of Things: a Survey," Journal of Future Generation Computer Systems, pp. 1-54, September2015.

[72] T. Bhattasali, R. Chaki, N. Chaki,, "Secure and trusted cloud of things". In: India Conference (INDICON), 2013 Annual IEEE, pp. 1–6.

[73] Y. Simmhan, A. G. Kumbhare, B. Cao, V. Prasanna, "An analysis of security and privacy issues in smart grid software architectures on clouds", In: Cloud Computing (CLOUD), IEEE International Conference on. IEEE, pp. 582–589, 2011.

[74] N. Grozev, R. Buyya, "Inter-cloud architectures and application brokering: taxonomy and survey", Software: Practice and Experience, vol. 44, issue: 3, pp. 369–390, 2014.

[75] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, S. V. Sharma, "Cloud computing for Internet of Things & sensing based applications", In: Sensing technology (ICST), 2012 Sixth International Conference on. IEEE, pp. 374–380, 2012.

[76] W. He, G. Yan, L. D. Xu, "Developing vehicular data cloud services in the iot environment", IEEE Transactions on Industrial Informatics, vol. 10, issue: 2, pp. 1587–1595, May 2014.
[77] C. Dobre, F. Xhafa, F., "Intelligent services for big data science", Future Generation Computer Systems, vol. 37, pp. 267–281, 2014.
[78] G. Aceto, A. Botta, W. de Donato, A. Pescap`e, "Cloud monitoring: A survey", Computer Networks, vol. 57, issue: 9, pp. 2093–2115, 2013.

Published Work in International Conferences

Published Work 1

Security and Privacy of Big Data for Social Networking Services in Cloud

Authors: Christos Stergiou, **Andreas P. Plageras**, Kostas E. Psannis, Theofanis Xifilidis, and Brij B. Gupta.

Abstract: Big Data (BD) is of great importance especially in wireless telecommunications field. Social Networking (SNg) is one more fast-growing technology that allows users to build their profile and could be described as web applications. Both of them face privacy and security issues. In this paper, we survey SNg, BD and Cloud Computing (CC) technology and their basic characteristics, by concentrating on the security issues of those technologies. Specifically, we aim at combining the functionality of these two technologies (i.e Big Data and Social Networking) in a CC environment, so that we can analyze the common features and ascertain the advantages of their integration related to security issues. Through this research, we present a new system-framework-network in Cloud Environment through which users of various Social Networks (SNs) will be able to exchange data and information, and primarily large-scale data (Big Data). With our proposed system, we can achive greatly improve of the communication of SN users, and thus become more safe and accurate in a Cloud environment. More specifically, this system could be established as an intermediate communication node that could be utilized in order to improve the security of SNg's users through the use of algorithms that can provide more privacy in the data related to BD technology. Also, in this work we present some measurements and results relative to our proposed system use. Finally, the opportunity to create a database through which each user can view the statistics of his interaction with the SNg is further discussed.

Keywords: Cloud Computing, Big Data; Social Networking; Framework; System; Security; Privacy;

I. INTRODUCTION

SN is a structure consisting of sets of social, dyadic ties, and other social interactions between people. The SN perspective offers a set of methods for analyzing the structure

of whole social entities as well as a variety of theories explaining the patterns observed in these structures [1]. SNs are "self-organizing, emergent, and complex, such that a globally coherent pattern appears from the local interaction of the elements that comprise the system" [2] (figure 1). Privacy concerns with SNg services is a subset of data privacy, involving the right of mandating personal privacy concerning storing, re-purposing, provide to third parties, and displaying of information connected with oneself through the Internet [3].

Fig. 1. Social Networks Society.

CC constitutes a technology of internet services providing remote use of hardware and software. As a consequence, the users of CC could have access to information and data from any place at any time. In recent years, giant companies of the IT and software sectors investigate the services of CC. Furthermore, another technology which generated relaying on CC is "Mobile Cloud Computing" (MCC). MCC based on the concept of the "Cloud" provides any type of information and data by no matter of where and when through mobile devices. Through this relative technology the owners of the data on the internet could manage information everywhere and at any time. Also, MCC could make the mobile devices resourceful in terms such as computational power, memory, storage and energy. Considering this, MCC technology, and furthermore CC technology in general, could be settled as a base technology to operate other technologies such as BD and SNg [4] [5] [6].

A way in which the issues of data security and data privacy in SNs could be solved or could be depleted by the use of "Big Data Analysis Tools and Services". The big data describes the data sets that are large or complex for the traditional data processing applications which are incompetent. "Big Data is often related to the use of predictive analytics or a set of advanced methods (Big Data Analytics) with the aim to extract merit from the collected data" [7] [8]. From this scope it is perceptible that the big data are now equally important both for business and internet. This happens because more data packets demand a more accurate analysis. Data analysis is a do-or-die requirement for today's businesses. The vendor community is responding by providing highly distributed architectures and new levels of memory and processing power [9] [10] [11].

The rest of the paper is divided in sections as follows. In Section 2 discusses in detail the technology of SNg and some of its basic characteristics about its security and privacy issues. Moreover, section 3 presents and analyzes the BD technology, and some basic information about its functionality. In Section 4, the proposed method of the paper

is presented and some useful information related. Section 5, presents the proposed system-framework-network. Finally section 6 provides the conclusions of the current paper, and sets the issues of future work.

II. SECURITY & PRIVACY FOR SNG

Social Networks can be described as web applications that permit users to create their semi-public profile [12] [13]. Most people join SNs to dispense their data and keep in contact with people that they are aware with. The main feature of SNs is a friend finder that allows SN users to search for people that they know and then build up their own online community [14].

Most SN users share a big amount of their private information in their social network space. A large number of users share their information publicly without careful consideration. Consenquently, SNs have become a large set of sensitive data. Moreover, SN users tend to have a high level of trust toward other SN users. They tend to accept friend requests easily, and trust items that friends send to them [15] [16].

Privacy and security issues on SNs are the most popular problems. The web-sites usually suffer from such problems. Meanwhile, security and privacy issues are entirely different problems. On the one hand, security issues occur when hackers gain unauthorized access to a site's protected coding or written language. On the other hand, privacy issues, those involving the unwarranted access of private information, do not necessarily have to involve security breaches. Confidential information such as typing a password can be revealed to anyone. But both types of breaches are often intertwined on SNs, especially “since anyone who breaches a site's security network opens the door to easy access to private information belonging to any user” [17] [18].

A. Social Networking Third-Party Output

Simple solutions are proposed for providing privacy when a SN uses third-party output. By these solutions personal data can be protected, but third party applications need direct access to the social graph information embodied in the user’s friend list. More specifically, the solutions can be separated in three categories [18]: 1) Data Hiding, 2) User Identification, 3) Public Data.

III. BIG DATA

BD is a more complicated world because the scale is much larger. The information is usually shared over a number of servers, and the work of compiling the data must be correlated among them. In the past, the work was largely delegated to the database software, which would use its magical JOIN [19] mechanism to compile tables, then add up the columns before handing off the rectangle of data to the reporting software that would paginate it. Database programmers can inform the users about the procedure about complicated JOIN commands that would lock up their database for hours as it tried to produce a report for the boss who wanted his columns just so [19] [20] .

BD sets advanced analytic techniques in which they operate on, that called BD Analytics. Therefore, BD analytics is about two things, BD and analytics, plus how the two have teamed up to produce one of the most profound trends in business intelligence (BI) today. Analytics helps us discover what has changed and how we should react [21] [22].

A. BD Features

Most definitions of BD focus on the size of data in storage. Size matters, but there are other important attributes of BD, namely data variety and data velocity. The three Vs of BD, which are volume, variety, and velocity, constitute a broad definition, and they bust the myth that BD is only about data volume. More specifically, each one of these three Vs has its own ramifications for analytics [21].

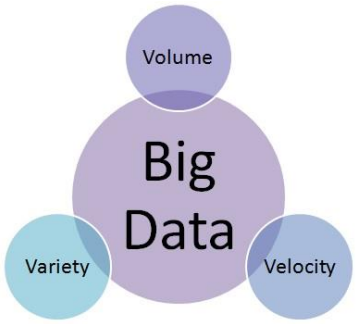


Fig. 2. The Three Vs of Big Data.

1) Big Data Volume
2) Big Data Velocity
3) Big Data Variety

B. BD Analysis Tools and Services

BD is the emerging discipline of capturing, storing, processing, analysing and visualising these huge quantities of information. The data sets may start at a few terabytes and run to many petabytes, far more than traditional data analysis packages can handle [23] [24].

Some BD tools that analyzed bellow are: 1) Jaspersoft BI Suite, 2) Pentaho Business Analytics, 3) Karmasphere Studio and Analyst, 4) Talend Open Studio, 5) Skytree Server, 6) Tableau Desktop and Server, 7) Splunk.

C. Big Data's impact in SNg

As the BD technology grows and spreads on the internet, many web technologies and applications that rely on it are affected. One of the many applications which are affected by the growth of the BD technology is the SNg.

TABLE I.

Big Data's characteristics affect on Social Networking's third party output.

Big Data Characteristics	Big Data Volume	Big Data Velocity	Big Data Variety
Data Hiding	**X**	**X**	**X**
User Identification	**X**	**X**	
Public Data	**X**		**X**

Table 1 lists the characteristics that the BD technology has, regarding the convenience that this technology offers, and on the other hand lists three categories of the SNg third party output. The aim of the Table 1 is to show how the characteristics of the BD technology are related to the the three categories of Big SNg third party output, and additionally how they affect these three categories. The conclusion that can be drawn from Table 1 is that the BD Volume affects more in the SNg third party output. We reach to this conclusion relying to our study on Big Data technology, and in addition the findings and the conclusions of the related works, which we have studied.

TABLE II.

Social Networking's third party output categories affect on Big Data's Analysis Tools & Services**.**

Big Data Analysis Tools & Services	Data Hiding	User Identification	Public Data
Jaspersoft BI Suite		**X**	**X**
Pentaho Business Analytics	**X**		**X**
Karmasphere Studio and Analyst			**X**
Talend Open Studio		**X**	**X**
Skytree Server	**X**	**X**	**X**
Tableau Desktop and Server	**X**	**X**	
Splunk		**X**	**X**

Table 2 lists three categories of the SNg third party output and on the other hand lists the Big Data's Analysis Tools & Services that we have studied in this paper. The aim of Table 2 is to show how the three categories of the SNg third party output related and affect the Big Data's Analysis Tools & Services. As shown, Table 2 demonstrates that the Public Data category are related more with the Big Data's Analysis Tools & Services which we have studied here. Also, another conclusion that can be drawn from Table 2 is that the Skytree Server was affected more by the three categories of the SNg third party output.

D. BD Security Issues

New challenges and standards developed and created in data security issues through the development and the use of BD technology. This creates a growing need for further research on security technologies in order to make handling the huge amount of data feasible and to ensure effectiveness. Technologies for securing data are slow when applied to huge amounts of data [25].

TABLE III.

Encryption Rates of popular Algorithms.

Algorithm	Key length	MB processed	Block size	Rounds	Time Taken	MB per Second
Blowfish	32-448 bits	256	64 bits	16	3,976	64,386
DES	56 bits	128	64 bits	16	5,998	21,340
3DES	56, 112 or 168 bits	128	64 bits	48	6,159	20,783
AES	128, 192 or 256 bits	256	128 bits	10, 12 or 14	4,196	61,010
RSA	1024-4096 bits	300	512 bits	1	1175,7826	10,900

Regarding Table 3, the conclusion that even the most efficient algorithms give an encryption rate of 64.3MB/s is reached. So, in the sector of BD technology, in which the need of large amounts of data to be transferred, we can confirm a significant bottle neck for encryption such large amounts data. This is detrimental to the nature of BD which have real time processing and results.

IV. EVALUATION EXPERIMENTS

As the BD technology develops and engages with other technologies, established new requirements result relating to operation and needs. Thus there exists a causality of BD technology with an equally growing technology over the last years, which is the the Social Networking.

Having studied some encryption algorithms regarding security issues of BD technology we find that with regard to security issues involving BD technology in SNg technology, there are some issues which can be combined in a Cloud Environment. Selecting two of the encryption algorithms that were previously studied, we attempt to modify them so they can be use data from the algorithms we use in the SNg technology with the aim to realize some specific measurements of the data can be obtained, and why not do it in a safer way. The two algorithms are selected based on their potential to receive more data per second. The algorithms are the Blowfish (64,386MB/s) and the AES (61,010MB/s).

Regard the Blowfish algorithm we can take the NIter, which is the maximum number of iterations with the aim to use it in the encryption algorithm, and to improve the security of the four different bio-inspired algorithms.

void encrypt (NIter & L, NIter & R) {…}
void decrypt (NIter & L, NIter & R) {…}

Regarding the AES algorithm we can take the same value, the NIter, which is the maximum number of iterations in order to use it in the encryption algorithm, and to improve the security of the four different bio-inspired algorithms.

int mbedtls_aes_crypt_ecb(NIter *ctx, int mode, const unsigned char input[16], unsigned char output[16]) {…}

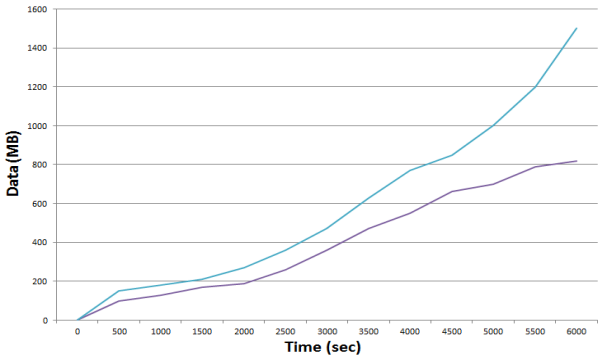


Fig. 3. Security level of encryption algorithms of measurement used for the study of four bio-inspired algorithms.

Figure 3 shows, the measurements with respect to time. As can be deduced by this figure the more often the combined use of the algorithms, the higher the level of security of the data we achieve every time. The upper line represents the Blowfish algorithm and the other (down line) represents the AES algorithm. More specific, Figure 3 could demonstrate a comparison of the implementation and the use of the two aforementioned encryption algorithms. The graph represents that through time the encryption procedure become more accurate and more efficient.

Regarding the Encryption Rate of the Transmitted Data the following equation is considered: the related work we derive the following equation:

$$E_n R_a = \frac{\mathrm{R_e}\, D_{ata} - \left(T_r D_{ata} * NI_{ter}\right)}{T_r T_{ime}} \qquad (1)$$

where,

Acronym	Description
E_nR_a	Encryption Rate of Data
R_eD_{ata}	Received Data
T_rD_{ata}	Transmitted Data
NI_{ter}	Maximum number of iterations
T_rT_{ime}	Transmission Time of Data sent

By applying, so equation (1), the following chart occurs.

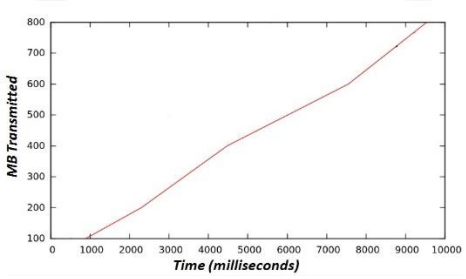


Fig. 4. Encryption Rate (Data in Time).

As observed from Figure 4, the encryption rate has an upward trend over time, in respect of data transmitted on the network. So, we can conclude that we need a good implementation of the encryption process mainly before sending the data, and then later in the transmission process.

Counting on the data packet switching procedures and use of the data on the internet, you need to make a further study of additional technologies, such as Internet of Things (IoT), in order to see if combined we can achieve better results on data usage and security issues [26] [27].

V. PROPOSED SYSTEM

Considering the study conducted for the related review, we can conclude that creating a system-framework-network in a “safe” Cloud environment through which users of the various Social Networks will be able to exchange data and information, and primarily large-scale data (Big Data), could greatly improve the communication of SN users.

In addition, having studied the available ways of security and authentication offered by social network providers, we reached that the system that we propose should work with authentication (sign in) through the account that will every user have in a SN (e.g. Facebook, LinkedIn YouTube, Instagram). In this way, each user will be able to connect to a more secure "private" network through which the user can exchange data in a “Safe Cloud Server” with other SN users, such as photos (mainly high quality) and videos (mostly high quality).

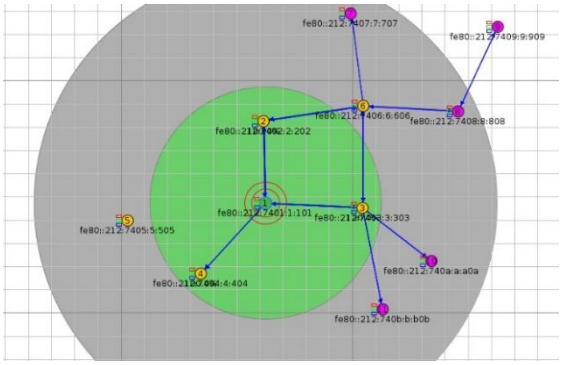


Fig. 5. Propoesd System’s Topology.

Having concluded that many similar technologies in the telecommunications sector can be combined with each other from the earlier study we have done, the network we created will be based, in terms of design, architecture, topology, on IoT technology. This type of network that we propose could be count on previous work of C. Stergiou et al [28], where a new type of network topology have been proposed (figure 5) in order to transmit high quality videos. Also, users of this network will be able to

exchange and other types of data such as personal files, which can be quite large. Users of the network will also be able to temporarily store data, as well as back up data, during the transmission process in a network space, based on CC technology. For multimedia data (Big Data) transfer within the network a protocol that has been proposed in a previous work of G. Kokkonis et al [29] will be used, the NAMRTP.

The proposed network system will use existing models of cryptographic algorithms to secure the authentication and data exchange process. Of course, there are some improvements - changes to some pieces of their source code, as we have seen in the previous section. The aim concerning the network will be to offer an alternative and more secure data exchange solution among users of SNs.

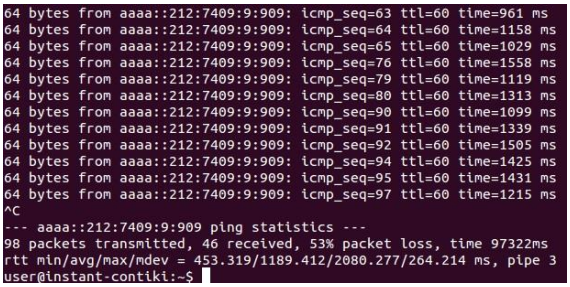


Fig. 6. Packets send throug Network (sample node 9).

Figure 6 shows the transmission procedure of packets sent through the network. As easily observed, each file that ends through the proposed network is divided to smaller packets of data in order to be sent. Regarding the large amount of data sent we have a small number of Packet Loss. More specifically, the node 9 which is shown in figure 6 is the most distant node of the simulation network.

$$P_aL_o = \frac{\left(P_aT_r - P_aR_e\right) - D_uP_a}{T_rT_{ime}} \qquad (2)$$

$$\frac{P_aR_e}{T_rT_{ime}} = \frac{P_aT_r - P_aL_o - D_uP_a}{T_rT_{ime}} \qquad (3)$$

where,

Acronym	Description
P_aL_o	Packets Loss
P_aT_r	Packets Transmitted
P_aR_e	Packets Received
D_uP_a	Duplicated Packets
T_rT_{ime}	Transmission Time of Packets sent

The (2) shows the Packet Loss of the transmission procedure through the proposed network. The rate of the Packet Loss differs through time and depends by the various amount of data send each time. While, on the other hand, (3) shows how the Packages Received during the Transmission process (Time) depend, from the Total Packets Transmitted, removing the Packet Loss and the Duplicated Packets, and dividing them by the Transmission Time.

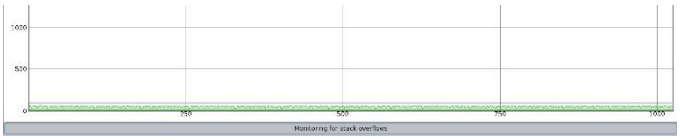


Fig. 7. Stuck overflow not detected.

Figure 7 demonstrates that there is no stuck overflow during the transmission procedure, so we can deduce that the whole process is smoothly carried out in the network.

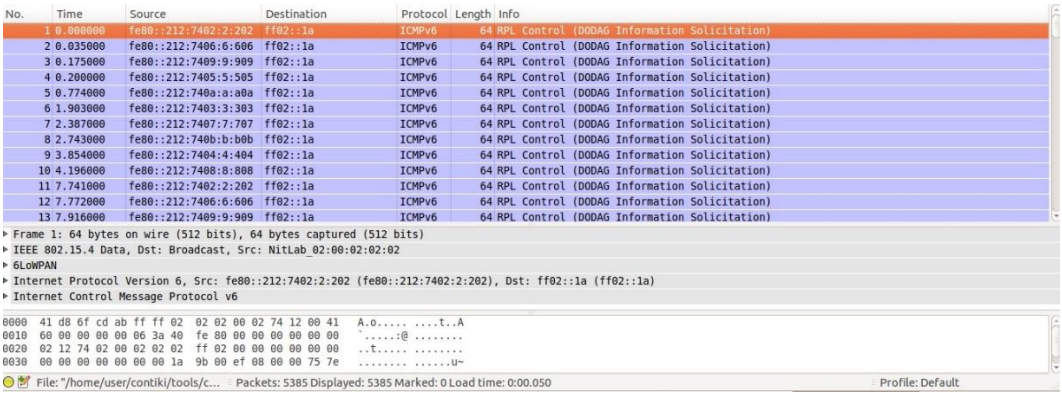


Fig. 8. Transmission proccess (a).

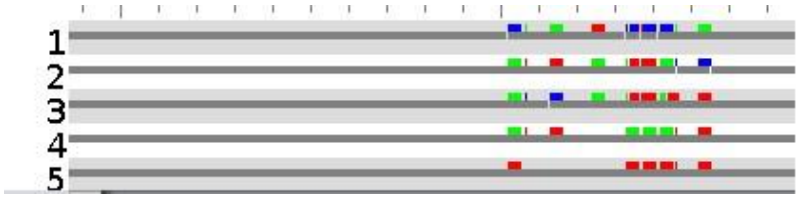


Fig. 9. Transmission proccess (b).

Figures 8 and 9 show the Transmission Packets procedure through the network. As observed, various types of packets were sent in the network by a number of connected users.

VI. CONCLUSIONS

SNg technology offers many possibilities, but also places several limitations as well. Social Networking could be described as web applications that allow users with the aim to create their semi-public profile. In the current work, we survey SNg, BD and Cloud Computing (CC) technology and their basic characteristics, with a focus on the security issues of those technologies. Additionally, we presented the basic characteristics of BD an SNg technologies, and also the major privacy and security issues that both technologies face. Subsequently and in terms of BD technology, we survey the algorithms with big impact to its security, and we present the basic characteristics of them.

Finally, we discuss the opportunity to create a database through which each user can see the statistics of his interaction with the SNg. The main goal of this paper is to try to combine the functionality of the BD and SNg technologies in a CC environment, in order to examine the common features, and also to discover the benefits related in security issues of their integration. Also, by examining their integration and functionality we could establish a new system-framework-network in Cloud Environment that combines these technologies, and some other technologies (e.g. IoT) related. This could be take place by presenting a new system-framework-network through which users of the various Social Networks will be able to exchange data and information, and primarily large-scale data (Big Data) and greatly improve the communication of SN users, and thus become more safe and accurate in a Cloud environment. Meanwhile, this system could be used for the purpose of improving security of SNg users through the use of algorithms that can provide more privacy in the data related to BD technology in a Cloud Server. This method is presented here and also some measurements results of its use.

This can be a field of future research on the integration of those technologies, and also have a huge improvement of their security and privacy issues. In addition to this, we can conclude that it would be a useful opportunity to create a database through which each user can see the statistics of his interaction with the SNg. Furthermore, based on the rapid development of network technologies the plethora of new technologies in this field, it would be good a further study to consider related technologies such as IoT, as a new case study.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and feedback which was extremely helpful in improving the quality of the paper.

REFERENCES

[1] S. Wasserman, K. Faust, “Social Network Analysis: Methods and Applications”, Urbana-Champaign: Cambridge University Press, pp. 1-27, March 1995.

[2] M. Newman, A.-L. Barabasi, D. J. Watts, “The Structure and Dynamics of Networks”, ACM, Princeton University Press Princeton, NJ, USA, 2006.

[3] C. Fabiana, M. Garetto, E. Leonardi, “De-anonymizing scale-free social networks by percolation graph matching”, in Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM), Kowloon, Hong Kong, 26 April-1 May 2015.

[4] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, December 2016.

[5] S. Sakr, A. Liu, D. M. Batista, & M. Alomari, “A survey of large scale data management approaches in cloud environments”, IEEE Commun. Surveys & Tutorials, vol. 13, no. 3, pp. 311–336, 2011.

[6] C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley Online Library, International Journal of Network Management, vol. 27, issue 3, pp. 1-12, May 2016.
[7] M. Hilbert, P. Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information", Science, vol. 332, issue: 6025, pp. 60-65, April 2011.
[8] Z. Fu, K. Ren, J. Shu, X. Sun, F. Huang, "Enabling Personalized Search over Encrypted Outsourced Data with Efficiency Improvement", IEEE Transactions on Parallel and Distributed Systems, vol. 27, issue: 9, September 2016.
[9] W. Culhane, K. Kogan, C. Jayalath, P. Eugster, "Optimal communication structures for big data aggregation", in Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM) , Kowloon, Hong Kong, 26 April-1 May 2015.
[10] A. Detsounis, G. S. Paraschos, I. Koutsopoulos, "Streaming big data meets backpressure in distributed network computation", Computer Communications, in Proceedings of 35th Annual IEEE International Conference on IEEE INFOCOM 2016, San Francisco, CA, USA, 10-14 April 2016.
[11] Z. Su, Q. Xu, Q. Qi, "Big Data in Mobile Social Networks: A Qof-Oriented Framework", IEEE Network, February 2016.
[12] T. Ma, J. Zhou, M. Tang, S. Lee, "Social network and tag sources based augmenting collaborative recommender system", IEICE Transactions on Information and Systems, vol. E98-D, no.4, pp. 902-910, April 2015.
[13] L. Bilge, T. Strufe, D. Balzarotti, E. Kirda, "All your contacts are belong to us: automated identity theft attacks on social networks", in Proceedings of the 18th international conference on World Wide Web WWW '09, pp. 551-560, Madrid, Spain. 20-2 April 2009.
[14] J. L. Z. Cai, M. Yan, Y. Li., "Using crowdsourced data in location-based social networks to explore influence maximization", in Proceedings of the 35th Annual IEEE International Conference on Computer Communications IEEE INFOCOM 2016, San Francisco, CA, USA , 10-14 April 2016.
[15] P. Chaudhary, B. B. Gupta, S. Gupta, "Auditing Defense against XSS Worms in Online Social Network-Based Web Applications," Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, IGI-Global's Advances in Information Security, Privacy, and Ethics (AISPE) series, USA, 2016.
[16] J. Cheng, Y. Zhang, Q. Ye, H. Du, "High-precision shortest distance estimation for large-scale social networks", in Proceedings of the 35th Annual IEEE International Conference on Computer Communications, IEEE INFOCOM 2016, San Francisco, CA, USA, 10-14 April 2016.
[17] D. Gunatilaka, "A Survey of Privacy and Security Issues in Social Networks," CSE571S: Network Security, pp. 1-12, November 2011.
[18] L.Yan, H. Shen, K. Chen, "TSearch: Target-oriented low-delay node searching in DTNs with social network properties", in Proceedings of 2015 IEEE Conference on

Computer Communications (INFOCOM) , Kowloon, Hong Kong, 26 April-1 May 2015.
[19] P. Wayner, "7 top tools for taming big data," InfoWorld, 18/4/2012. [Online]. Available: http://www.infoworld.com/article/2616959/big-data/7-top-tools-for-taming-big-data.html. [Accessed 21/5/2016].
[20] A. P. Plageras, C. Stergiou, G. Kokkonis, K. E. Psannis, Y. Ishibashi, B.-G. Kim, B. B. Gupta, "Efficient Large-scale Medical Data (eHealth Big Data) Analytics in Internet of Things", in Proceedings of 2017 IEEE 19th Conference on Business Informatics (CBI), International Workshop on Internet of Things and Smart, Thessaloniki, Greece, 24-26 July, 2017.
[21] Cloud News Daily, "Guide to Big Data Analytics: Platforms, Software, Companies Tools, Solutions and Hadoop," Cloud News Daily, 12/12/2015. [Online]. Available: http://cloudnewsdaily.com/big-data-analytics/. [Accessed 21/5/2016].
[22] K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, W. Xiang, "Big Data-Driven Optimization for Mobile Networks toward 5G", IEEE Network, February 2016.
[23] S. Kaisler, F. Armour, J. A. Espinosa, W. Money, "Big Data: Issues and Challenges Moving Forward", in Proceedings of 2013 46th Hawaii International Conference on System Sciences (HICSS), pp. 995-1004, Wailea, Maui, HI, USA, 7-10 January 2013.
[24] K. Raichura, N. Padhariya, "BigCache: a cache-based Big Data management in mobile networks", International Journal in Mobile Communications, vol. 15, no. 1, pp. 49-68, 2017.
[25] C. Stergiou, K. E. Psannis, "Algorithms for Big Data in Advanced Communication Systems and Cloud Computing", in Proceedings of 2017 IEEE 19th Conference on Business Informatics (CBI 2017), Thessaloniki, Greece, 24-26 July 2017.
[26] C. Stergiou, K. E. Psannis, "Efficient and Secure Big Data delivery in Cloud Computing", Springer, Multimedia Tools and Applications, vol. 76, issue 21, pp. 22803–22822, November 2017.
[27] K. Yang, X. Jia, K. Ren, R. Xie, L. Huang, "Enabling efficient access control with dynamic policy updating for big data in the cloud", in Proceedings of 2014 IEEE INFOCOM, Toronto, ON, Canada, 27 April-2 May 2014.
[28] C. Stergiou, K. E. Psannis, A. P. Plageras, Y. Ishibashi, B. B. Gupta, B.-G. Kim, "Architecture for security monitoring in IoT environments", in Proceedings of 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, Scotland (UK), 19-21 June 2017.
[29] G. Kokkonis, K. E. Psannis, M. Roumeliotis, D. Schonfeld, "Real-time wireless multisensory smart surveillance with 3D-HEVC streams for internet-of-things (IoT)", Springer, Journal of Supercomputing, vol. 73, issue: 3, pp. 1044-1062, March 2017.

Published Work 2

Proposed High Level Architecture of a Smart Interconnected Interactive Classroom

Authors: C. Stergiou, **A. P. Plageras**, K. E. Psannis, T. Xifilidis, G. Kokkonis, S. Kontogiannis, K. Tsarava, and A. Sapountzi.

Abstract: This paper presents the high level architecture of a smart, modern, interactive laboratory-class called Smart Interconnected Interactive Classroom (SIIC). It describes the interoperability of telecommunication technologies, sensors and actuators over a virtual environment that enhances the learning process and experience. In the context of this work novel augmented and virtual services are outlined that can assist e-Learning systems through virtual reality and real-time interactions.

Keywords: Smart Classroom; Haptic technology; Cloud services; Internet of Things; Big Data; middleware protocols; virtual reality

I. INTRODUCTION

Educational Learning Management systems (LMS), are of high impact in terms of technology appliance and testing methodologies. Although the field of smart-Education has been scientifically established, it is currently in an embryonic 2D data representational state. Contemporary LMS systems include components such as Forum, Wiki, knowledge surveys, tasks, document management, games, reporting that assist teaching process. These aggregations of services are part of the asynchronous LMS functionality, while the use of VoD services, and real-time, mobile audio-video course conducting services are part of the synchronous LMS functionality [13- 15]. In this paper the authors propose the incorporation of 3D virtual services in an LMS platform that will include both synchronous and asynchronous services into the virtual class. Furthermore, the proposed virtual class will utilize sensors and haptic equipment [11] together with state-of-the-art hardware implemetation and sensors in order to carry out augmented human sensing information and touch into the virtual class.

Hence, based on the above, the application of technologies mentioned for the implementation of the proposed Smart Interconnected Interactive Classroom (SIIC) constitutes an ambitious step and a perspective that will inaugurate progress in the first and second grade education [8-10]. The proposal of this paper must be fully aligned to software solutions accompanied by advanced hardware solutions that efficiently support the services provided. The proposed SIIC architecture is presented at section II. At section III, the authors outline proposed novel services and protocols that will embrace virtuality, while at section IV, the authors present considerations and implementation plan.

Internet of Things (IoT), Big Data (BD) and cloud technologies are already well-established and have progressed rapidly, counting many years of life and scientific interest [1, 3]. In the Cloud Services (CS) field, data compression and delay tolerant

data representation is relatively more recently spread out because of the IoT technological outburst.

Regarding the aforementioned technologies, starting with Cloud Computing (CC), it is consisted as a technology of internet services providing remote use of hardware and software. Thus, the users of CC could have access to information and data from any place at any time. CC in general, could be settled as a base technology to operate other technologies such as Internet of Things and Big Data. Moreover, we could realize that the basic idea of the IoT is the pervasive presence of a variety of things or objects used by people such as radio-frequency identification tags, sensors, actuators, and mobile phones. Finally, as regards the Big Data, we could define that it is a new popular term, used to describe the surprisingly rapid increase in volume of data in structured and unstructured form. BD usually uses Cloud Computing (CC) as a base technology in order to operate [1-3].

Wireless communications include technologies and equipment for data collection from wireless sensors, such as temperature, smoke, humidity, capacitive touch, and task instructed communication protocols such as streaming, real- time, interactive, responsive and best effort. At this point, it should be noted that the sensor network efficiency must be carefully addressed as to ensure reliable data gathering. Hence, the network topology must comply to the location of the indoor-smart classroom user terminals and the main factors of signal degradation and attenuation. This aggregation of devices and specialized protocols connected to the Internet cloud and focused only to a specific user is part of the immersing revolution of cloud-oriented, multi-disciplinary user targeted services, named after the nickname smart [2]. It is a fact that concerning that state-of-the-art technology Greece is not highly ranked. Thus, as the transition to the state-of-the-art 5G networks is realized and specifically considering indoor application, the convergence of the aforementioned technologies combined with smart technology is at the center of scientific interest [5-7]. Moreover, contemporary BLE, LoRa and XBee low power networking technologies for sensory data acquisition are still not fully exploited. In addition, obsolete technologies of 2G/3G and SCADA-RTU/smart equipment communication protocols (DNP3, Modbus, Ethernet IP based IEC 61850, IEC60870, RS232/Parport EPICS). Even SCADA systems nowadays, with the development of IoT and cloud technology are moving towards that adoption.

Virtual reality is a known scientific area of high interest. Combined with the Haptic sense and haptic protocols for haptic data transfer via Internet, the proposed system will provide capabilities of conducting experiments in courses such as Physics and using on-line applications in an interactive distance learning [11, 12]. The students will have the capability of developing active learning and improving their knowledge level, while at the same time motivation will be provided from the teacher as well as the interconnected interactive technology itself, thus contributing to the overall improvement of their educational and technological training level. Moreover, the students, being part of this virtual smart interactive classroom will gain better understanding of the concepts presented in the courses and develop useful skills and

abilities of solving complex problems. The appliance of the proposed architecture in every school in first and second grade education will have a significant impact as it will improve education quality with long-term benefits in the educational level and the scientific training of young scientists.

II. LITERATURE REVIEW

For the purpose of this work we count on previous literature works which has been published in the related field. The following paragraphs present the papers which contributed significantly in our study.

In [1] the authors survey BD and CC technology and their basic characteristics, with a focus on the security and privacy issues of both technologies. Particularly, the authors try to combine the functionality of the two technologies with the aim to examine the frequent features, and also to discover the benefits related in security issues of their integration.

Additionally, this work presents a new method of an algorithm that can be used for the purpose of improving Cloud Computing's security through the use of algorithms that can provide more privacy in the data related to BD technology.

The [3] presents a survey of IoT and Cloud Computing with a focus on the security issues of both technologies. More specifically, the authors try to combine these two technologies with the aim to examine the common features, and in order to discover the benefits of their integration. Through this work, it is shown how the Cloud Computing technology improves the function of the IoT.

The [4] presents related work on High-Efficiency Video Coding. It points out the challenges and the synchronization techniques that have been proposed for synchronizing video and haptic data. Resulting, the [4] proposes a new efficient algorithm for transferring a real-time HEVC stream with haptic data through the Internet.

The authors of [9] try to attempt the evaluation of an educational scenario, where the implementation of which is based on Cloud Computing tools that serve collaborative learning. The aim of the collaborative activities of the script is to understand and consolidate the usefulness of the criteria that make an educational video appropriate or not, for its introduction into the educational process.

The [14] describes the use of data mining techniques, such as clustering, classification, and association, in order to analyze the log file of an e-Learning platform and deduce useful conclusions. Also, a case study based on a previous approach was applied to e-Learning data from a Greek University.

III. ISIIC HIGH LEVEL SYSTEM ARCHITECTURE

The authors propose a novel system architecture over a virtual reality world (realm) and define the services that will support user-real interaction. This virtual architecture will support a virtual lab environment and it is called as Smart Interconnected Interactive Class (SIIC). The main objective of the proposition is to enhance learning process out

of the class boundaries, supporting user sense transfer, and distant interaction. Smart Interconnected Interactive Classroom is consisted of the following structural parts: a) Interactive interface workstations, equipped with Haptic equipment and sensors The architecture of each interactive interface workstation that comprises the interactive class user stations is illustrated at Figure 1.

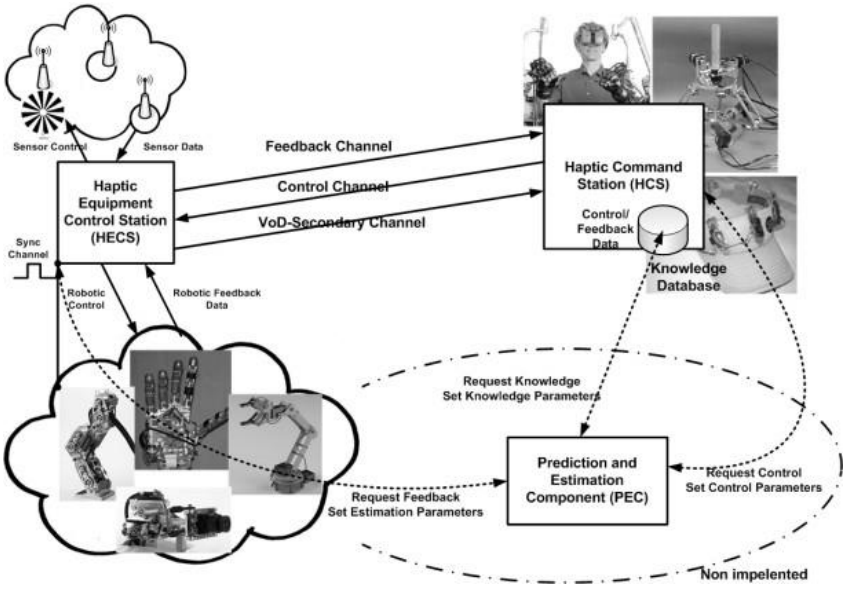


Fig. 1. Student interface system-workstation architecture of a workbench providing enhanced and interactive virtual reality capabilities.

The practical implementation of such an interconnected environment can be realized with the direct-real-time networking capabilities enforcement among the instructor and the workstations equipped sensor-actuator devices (human machine interfaces) of his students. This requires the implementation of appropriate interactive and real-time protocols either at application level (for each of the aforementioned services separately) or at the interoperability of sensor systems and data transfer in the Learning Management System (LMS) [4, 17].

The proposed SIIC architecture will be comprised of the following: 1) a cloud computing server LMS (Learning Management System) which acquires periodically and real- time data streams of users, actuators and sensors, stored from a set of tactile devices and equipment inter-connected via a local wireless network. [15], 2) For the haptic devices data handling, appropriate application/data transfer protocols will be designed and implemented according to [4, 7, 12, 17] 3). Computer devices, haptic devices [11], virtual and augmented reality headsets, and student sensors will be installed in the proposed classroom in to each one workstation entity, where the testing of protocols and human-machine interoperability with the virtual world will be performed. A very promising scientific field is that of providing feedback which could significantly enhance quality of services based on the fact that future data requirements may be previously estimated based on frequently appearing patterns. The benefit is two-fold: the future network data processing could be considerably improved based on the

"memory" of the whole system and energy efficiency particularly concerning sensor limited battery-life could be achieved if prediction is performed off- line.

The instructor will also have online access to the modified LMS system and equipped with virtual course capabilities and interfaces with the virtual class. The modified product will be named as LMS system of Virtual Context (LMSVC), where user sensory data will be stored in real time or interactively during the course. In front of the LMSVC system a balancing controller shall be used [16] that will monitor user interaction, besides the data usage of the devices, sensors and actuators data that will be available for data mining and knowledge extraction. The LMSVC will offer the virtual creation and the previously mentioned interactive real-time virtual services, as well as the capabilities of conventional 2D-LMS systems, such as virtual Documents, virtual announcements, virtual self-evaluation virtual exercises, virtual works and questionnaires, forum wiki, etc.

These services of conventional LMS systems will be provided offline and distant (without the requirement of course conduction in the interactive class), in the virtual learning world where the student with the virtual reality headset can be connected to the LMS Virtual Balancer [16], download documents through his/her tablet, computer and assess LMS system services in a 3D visual sense [20]. The LMS application virtual services and data transfer protocols enclosed, as well as the pilot headset application that will interface the student to the LMSVC system will be implemented within the framework of the project.

The SIIC system will enable pupils to approach the scenes of the modern virtual educational process and to get in touch with modern supervisory tools. The social impact of SIIC will be particularly important, as First and Secondary Education will have access either to a physical presence or to the Internet in this experimental class. Students will understand through empirical learning, with the help of augmented reality. All students' interaction with the system will be recorded and new teaching methods will emerge through the study of such behavior.

IV. SERVICES OF THE SMART INTERCONNECTED INTERACTIVE CLASSROOM

The authors proposed virtual services to be tested and implemented within SIIC apart from existing synchronous and asynchronous services are the following:

1. Virtual classroom service. This service will enable the student to immerse in an interactive three dimensional environment of the class from artificial virtual imaging projected by the LMS system to the end user using 3D virtual reality equipment (VR-Box, VR-Glasses). The interaction between the user members (avatars) of this virtual class will be carried out from the real world to the virtual world through the use of tactile-haptic devices and appropriate 3D modeling and presentation layers. The network protocols that will support this service and the virtual illustration of existing LMS modules are the standard best-effort HTTP-TCP protocols for connection oriented

services, UDP protocols for text and messaging services and RTP-RTCP protocols as well as experimental ones for HEVC streaming services [7, 4].

2. Cognitive Service and Augmented sensory services. Augmented reality service will utilize sensors for monitoring user body activity and bio-readings [17]. Such readings will be transferred to the virtual world and will be illustrated to the virtual class and virtual user navigation among the virtual class facilities-LMS components (augmented-sense service). Energy conservation is a crucial optimization parameter for the wireless sensor as stated previously. Based on the authors' claim that this smart interactive classroom is built with state-of-the-art components and operations the sensors could benefit from energy harvesting methods which involve collecting energy from neighboring networks. Although this could prove costly it will prolong sensor life-time.

Augmented reality service will also provide in real time via EMG sensors, temperature sensors, sweat sensors, augmented information of the student's mental and psychological state. By using sensory data and implementing artificial intelligent and data mining algorithms with appropriate pattern profiles, can offer measurements of user mood indication and user level of course understanding. Such capabilities are part of the proposed cognitive service that will enable adequate supportive information like whether the student is interested, or understands the delivered content of the virtual lesson or if the user is not in a disordered attention state along with the user's current perception and course interest [8]. Also this cognitive service real-time reporting can be recorded and used as feedback by other student-course evaluation services [14]. Augmented reality and cognitive services will use protocols that offer asynchronous communications in the context of request and response such as the CoAP protocol. In cases of sensor measurements of periodic synchronous transmissions the MQTT protocol will be used. In addition, experimental protocols for periodic and asynchronous IoT devices, proposed by the authors for medical services will replace CoAP and MQTT as more efficient [1, 2, 3, 17].

3. Positioning service. This service will control the student's current position within the virtual class in contrast to its real-class indoor position. For the process of indoor positioning, a set of Wi-Fi / BLE transceivers (iBeacons) – will be used with the implementation of location-positioning algorithms in the LMS system that will provide the exact position-placement of the student inside the classroom projected to the virtual world. Positioning service will use two different types of protocols for data delivery of movements to the virtual world. Using a periodic synchronous protocol with no ACK feedback such as UDP for carrying little motion information and a high resolution stream protocol such as RTP accurate positioning due to collaborative activities is required [9, 17].

4. Touch interaction service-Haptic service. This service will provide the ability to visualize the sense of touch in the virtual world and experience the virtual touch of others in the real world. This service will be experimentally tested with the use of specially designed gloves equipped with appropriate analogue pressure sensors and infrared transceivers. This service will be used to interact with the classroom of visually

impaired people as well as to enhance users' experience through the sense of touch. This service will use low latency, better than best effort streaming protocols of high priority and feedback control [11, 12].

5. 3-dimensional design and modeling service. This service will enable the student to have his own virtual workshop where he can use object-oriented toolboxes to design objects. This service will enable the student through a 3d-scanner to transfer via scanning, matter of the real world in the ideal while using 3D printers to implement constructions of the ideal world [18].

6. Virtual reality recording service. This LMS service will provide audiovisual recording of the virtual classroom and classroom interactions using 3d user model avatars. Part of the virtual reality recording service is the On-demand playback holographic service of virtual reality context. This LMS service will offer on-demand content and 3d user actions either in the real or virtual world, by showing a past virtual reality recorded session. Part of the recording service, will also be the 3D avatar creation component and the 3D lab presentation module that will be used to project the virtual world to an external user by using projection equipment [18, 19].

7. Virtual course student assessment service. This service will use intelligent algorithms developed by this project as well as clustering-classification techniques upon sensory and haptic data of virtual class, or visual information recordings, in order to evaluate the response and overall performance of students in that class. The same service will be responsible for the delivery of course self-evaluations and overall student evaluation reports [13, 14].

Within the framework of the proposed interactive class, the teacher will be able to connect and interact through their students' laptops, tablets, mobile phones and interconnected sensors in an isolated and secure network. Table I summarizes the proposed virtual class services and protocols assigned per each service class.

Additionally, students will also be able to interact with each other in a virtual course and exchange information during that virtual course. The proposed system and implemented protocols will deliver a virtual classroom and real-to-virtual interaction, in which multiple interconnected new technologies will be securely integrated and the services protocols involved as specified per service will provide best effort deliveries, low complexity and high scalability.

TABLE I.
PROPOSED SIIC SERVICES AND PROTOCOLS UTILISED PER SERVICE SUMMARY TABLE

SIIC service	**Delivery Requirements**	**Protocolsused**

Virtual Class service	Virtual class 3D context-real-time Chat services – connectionless over HTTP or UDP LMS asynchronous components – connection oriented over HTTP LMS streams-synchronous components over RTP or HTTP	HTTP – TCP UDP RTP-RTCP NAFCA [4]
Cognitive Service and Augmented sensory services	Asynchronous unreliable Asynchronous reliable Periodic unreliable Periodic reliable	SNMP-UDP CoAP MQTT MESETP [17]
Positioning service	Differentiated-reliable stream, unreliable periodic	UDP RTP MESETP [17]

Our research has two key tools for verifying the reliability of the results and the progress of the research project. The first and fundamental tool for verifying the reliability of the results from our research as well as the progress made by the research team will be internal quality control. The internal quality control will be the main responsibility of the research team and will be carried out mainly by the Scientific Director of the Research, as well as by the collaborating institutions that will contribute to the realization of the specific project. The second and "final" tool, as could be described, is a tool for verifying the reliability of the results and the progress of the project is the external quality control, which will be carried out by the collaborators who can access the educational environments and implement "pieces" of the progressive development of the project.

Regarding hardware implementation and computing power along with computational burden, the integration of the aforementioned wireless technologies must be adjusted to constructing an indoor wifi Local Area Network consisted of its essential parts: a wireless network adapter, a wireless router with access points spread across the rooms of the building that facilitates the smart classrooms, proper types of antennas for indoor applications and multiple relays that aim to amplify the propagating signal to reach its destination with sufficient power.

The network adapter aims to improve network performance. The router accompanied by wireless protocols such as 802.11ac is an essential part. Wireless antennas increase the network coverage, while repeaters ensure successful file delivery.

A final remark concerning computational power efficient software solutions must be used together with hardware able to gather, compress and process data with the minimum computation power and burden.

VI. CONCLUSION AND FUTURE WORK

The key to achieving this proposal is the ability to develop an evolutionary study, since it will be possible to test what benefits a modern and interactive class can offer, with the specific characteristics and the specific mode of study, in teaching, with the help of specialized associates and team members. Thus, we will be able to contribute in the

improvement of the modern educational process, taking into account real scenarios and studies. In this way, we will be given the opportunity to gradually improve the final deliverable as it will be used in real learning conditions. Furthermore, as a case study for the future work of this project will be a smart-interactive laboratory-class and an educational software that can be used in more than one language. The statements above together with the following two paragraphs provide the straightforward benefits of applying the proposed technology.

The proposed SIIC system virtual services and protocols is an authors ongoing research project eligible for funding at ELIDEK (Hellenic Foundation for Research & Innovation) p.III.

This proposal will help pupils to come closer to the scenarios of the modern educational process and to come up with modern supervisory tools. Additionally, because of the "special" nature and laboratory equipment will be given the possibility for remote access to augmented - virtual reality [18-20] by educational institutions all over the world. In this proposed system architecture, there will be a plethora of educational tools/experiments that will use the augmented virtual reality to maximize the learning outcomes. Thus, schools of primary and secondary education will be able to connect to the augmented reality lab via the Internet from their school's computer labs with the help of their teachers, by the use of our propose system architecture.

The social impact of our proposal will be particularly important, as all schools in Primary and Secondary Education will be able to access either physically or online in this experimental laboratory-class. Also, knowledge will not only be acquired through the traditional teacher-centered way of teaching, but emphasis will be placed on experiential learning based on the modern equipment of the laboratory. In an educational learning scenario that we will deal with, a proactive role in experiential learning will be given to the sense of touch, using haptic devices [11], along with the sense of hearing and vision. All students' interaction with the system will be recorded and new teaching methods will emerge through the study of these behaviors.

REFERENCES

[1] C. Stergiou, K. E. Psannis, “Efficient and Secure Big Data delivery in Cloud Computing”, Springer, Multimedia Tools and Applications, vol. 76, issue: 21, pp. 22803–22822, November 2017.

[2] C. Stergiou, K. E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey", Wiley, International Journal of Network Management, pp. 1-12, May 2016.

[3] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, December 2016.

[4] G. Kokkonis, K. E. Psannis, M. Roumeliotis, Y. Ishibashi, “Efficient algorithm for transferring a real-time HEVC stream with haptic data through the internet”, Journal of Real-Time Image Processing,Volume 12, Issue 2, pp 343–355, August 2016.

[5] I. Kakalou I., K. E. Psannis, P. Krawiec, R. Badea, “Cognitive Radio Network and Network Service Chaining towards 5G: challenges and requirements”, IEEE Communications, September 2017.

[6] K. E. Psannis, “Radio Resource Allocation on Complex 4G Wireless Cellular Networks”, 4th International Conference on Mathematical Modeling in Physical Sciences, Session: Statistical Physics and Applications, Mykonos, Greece, June 5-8, 2015 (http://icmsquare.net/).

[7] K. E. Psannis, “Adaptive Layered Segment Algorithm for Media Delivery over 4G LTE Wireless Cellular Networks”, IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB2013), Brunel University, Uxbridge, West London, UK, June 2013.

[8] K. Tsarava, K. Moeller, N. Pinkwart, M. Butz, U. Trautwein, M. Ninaus, “Training computational thinking: Game-based unplugged and plugged- in activities in primary school”, Proceedings of the 11th European Conference on Game Based Learning (pp. 687-695). Reading, UK: Academic Conferences and Publishing International Limited, 2017.

[9] E. Markaki, K. Tsarava, "Collaborative Activities with Cloud Computing Tools for Teacher Training in the Educational Use of Youtube" (2015). 4th Panhellenic Scientific Conference “Integration and Use of ICT in the Educational Process”, 30th October-1st November 2015, Thessaloniki, Greece.

[10] K. Tsarava, S. T. Halkidis, P. Venardos, G. Stephanides, “ Teaching basic calculus using SAGE”. Strategic Role of Tertiary Education and Technologies for Sustainable Competitive Advantage, 2013.

[11] G. Kokkonis, K. E. Psannis, M. Roumeliotis, S. Kontogiannis, Y. Ishibashi, “Evaluating Transport and Application Layer Protocols for Haptic Applications”, IEEE International Symposium on Haptic Audio- Visual Environments and Games (HAVE2012), Munich, Germany, October 2012.

[12] G. Kokkonis, K. E. Psannis, M. Roumeliotis, S. Kontogiannis, “A Survey of Transport Protocols for Haptic Applications”, 16th Panhellenic Conference on Informatics (PCI 2012), Piraeus, Greece, October 5 - 7, 2012.

[13] I. Kazanidis, S. Valsamidis, S. Kontogiannis, A. Karakos, "Courseware Evaluation Through Content, Usage and Marking Assessment", Research on e-Learning and ICT in Education, Springer ISBN: 978-1- 4614-6501-0, Jun 2014, pp. 149-161, 2014.
[14] S. Valsamidis, S. Kontogiannis, I. Kazanidis, A. Karakos, "E-Learning Platform Usage Analysis", Interdisciplinary Journal of E-Learning and Learning Objects (IJELO), vol. 7, issue 1, ISSN 1436-4522 , Oct. 2011, pp. 185-204.
[15] S. Valsamidis, S. Kontogiannis, I. Kazanidis, T. Theodosiou, A. Karakos, "A Clustering Methodology of Web Log Data for Learning Management Systems", Journal of Educational Technology and Society (ETS), vol. 15, issue 2, ISSN 1436-4522 , Jul. 2012, pp. 154-167, 2012.
[16] S. Kontogiannis, A. Karakos, "ALBL: An Adaptive Load BaLancing algorithm for distributed web systems", International Journal of Communication Networks and Distributed Systems, vol. 13 issue 2, July 2014, pp. 144-168.
[17] D. Tomtsis, S. Kontogiannis, G. Kokkonis, I. Kazanidis, S. Valsamidis, "Proposed cloud infrastructure of wearable and ubiquitous medical services", in Proc. Of the 5th Internation conference on Digital Information Processing and Communications (ICDIPC), IEEE proceedings, pp 213-218, 2015.
[18] E. Gounopoulos, S. Kontogiannis, I. Kazanidis, S. Valsamidis, "A framework for the evaluation of multilayer web based learning", in Proc of 20th Panhelenic conference on Informatics (2016), ACM proceedings, ISBN:978-1-4503-4789-1, pp. 161-164, Nov. 2016.
[19] E. Gounopoulos, S. Kontogiannis, S. Valsamidis, I. Kazanidis, "Blended Learning Evaluation in Higher education courses", KnowledgeE, vol. 1, No. 1, pp. 385-399, ISSN: 2518-668X, 2017.
[20] I. Kazanidis, S. Valsamidis, S. Kontogiannis, A. Karakos, "Courseware Evaluation Through Content, Usage and Marking Assessment", Research on e-Learning and ICT in Education, Springer ISBN: 978-1- 4614-6501-0, Jun 2014, pp. 149-161.

Published Work 3

Architecture for Security in IoT Environments

Authors: C. Stergiou, K. E. Psannis, **A. P. Plageras**, G. Kokkonis, Y. Ishibashi

Abstract: The focus of this paper is to propose an integration between Internet of Things (IoT) and Video Surveillance, with the aim to satisfy the requirements of the future needs of Video Surveillance, and to accomplish a better use. IoT is a new technology in the sector of telecommunications. It is a network that contains physical objects, items, and devices, which are embedded with sensors and software, thus enabling the objects, and allowing for their data exchange. Video Surveillance systems collect and exchange the data which has been recorded by sensors and cameras and send it through the network. This paper proposes an innovative topology paradigm which could offer a better use of IoT technology in Video Surveillance systems. Furthermore, the contribution of these technologies provided by Internet of Things features in dealing with the basic types of Video Surveillance technology with the aim to improve their use and to have a better transmission of video data through the network. Additionally, there is a comparison between our proposed topology and relevant proposed topologies focusing on the security issue.

Keywords: Internet of Things; Video Surveillance; IoT; monitoring; network topology; architecture;

I. INTRODUCTION

A number of modern mobile devices, like mobile phones, PDAs, laptops and others, become ubiquitous in recent years and people into the era of pervasive computing [1]. All these devices could be used with the aim to find out useful information when we are on the road and when we are travelling. This procedure can help us to define monitoring. Thus, "Monitoring is the act of listening, carrying out surveillance on, and/or recording the emissions of one's own or allied forces for the purpose of maintaining and improving procedural standards and security, or for reference, as applicable" [2].

Regarding this definition it is proved that monitoring related to surveillance. So, also, we could define surveillance, as a related part of technology in this work. Surveillance is "the close observation of the behaviour, the activities, or other changing information" [3] [4]. Sensors and cameras or other compatible devices are necessary for the surveillance with the aim to do the monitoring. With the use of this technology observation at a distance is possible, using electronic equipment [4] or stealing electronically transmitted information which may include simple, relevant technology methods.

Furthermore, in telecommunication fields there is a new technology called Internet of Things (IoT) [5]. The next major step in the recent technology field is the IoT technology, but however with the major difference that brings enormous changes in business functionality [6] [7]. In order to fully exploit these two technologies, it is mandatory to combine them so as to achieve the optimisation of surveillance technology through the use of the Internet of Things technology [8] [9].

The rest of the paper is organised as follows. In section 2 there is a review of the related research which deals with the monitoring urban areas throw modern networks. Section 3 presents and illustrates the proposal of a contribution of the Internet of Things technology in the function of Video Surveillance with the aim to offer a new topology paradigm. In Section 4 there is a comparison between our proposed topology and other related proposed architectures-topologies. Finally, section 5 provides the conclusions of the current paper and offers new possibilities for the development of future work.

II. RELATED WORKS

For the purpose of this paper we study and analyse previous studies in monitoring urban areas throw modern networks and we examine existing work proposed both in the literature and on the Internet. Below presented the papers we have studied with their main objective.

There are various works for the monitoring urban areas throw modern networks. A large number of several works related to monitoring urban areas throw modern networks the last two years. To begin with, the authors of [10] introduces the Shadow Security Unit, a low-cost device deployed in parallel with a PLC or Remote Terminal Unit (RTU), being able to transparently intercepting its communications control

channels and physical process I/O lines with the aim to continuously assess its security and operational status. The device that proposed in [10], regarding the existing control network, does not require considerable changes, in order to be capable of work in standalone or integrated within an ICS protection framework. Also, by the work that has been made in [11], the authors propose an innovative approach for the development of software for modelling of decentralised intelligent systems for security monitoring and control in power systems. The novelty of [11] is to joint use the modern computing environments. Also, the proposed intelligent system was tested on the modified 53-bus IEEE power system. The main aim of [12] is to describe an innovative security system able to localise and classify audio sources in an outdoor environment. The primary intended use of the proposed security system is for security monitoring in serve scenarios, and it has been designed to cope with a large set of heterogeneous objects, including weapons, human speakers, and vehicles. Also, in [12] after the presentation of the details of the system's design, with a particular emphasis on the innovative aspects that are introduced with respect to the state- of-the-art, the authors offer an extensive set of simulations in order to show the effectiveness of the proposed architecture. At the end the authors conclude be describing the current limits of the system, and the projected further developments. The current knowledge in the regard of the use of different tools needed in order to monitoring atmospheric pollution extended in [13]. The chemical response of the lichen Ramalina celastri was evaluated through physiological parameters and sulfur accumulation in relation to the SO2 and NO2 concentrations present in the air at the monitoring sites with different emission sources, with the aim to assess the atmospheric pollution in urban environments. Regarding this, it was possible to create different levels of air quality using simultaneous measurements of gaseous pollutants in the air and of parameters for the exposed biomonitor, as well as to determine the relationship between them and their society with the different emission sources present. In addition, in [14] discussed that in regions with a mild climate, pesticides are often used around homes for pest control. Pesticide use in residential areas linked to aquatic toxicity in urban surface water ecosystems, and suggested dust particles on a paved surface as an important source of pesticides by the recent monitoring studies which have been made. With the aim to be tested the hypothesis that dust on hard surfaces is a significant source of pesticides; the authors of [14] evaluated spatial and temporal patterns of current-use insecticides in Southern California, and further explored their distribution as a function of particle sizes.

The [15] reports on the first results of a long-term UFP monitoring network, set up in Amsterdam (NL), Antwerp (BE), Leicester (UK) and London (UK), with the aim to gain a better understanding on the spatiotemporal alteration of ultrafine particles (UFPs) in urban environments. Furthermore, the authors of [15] in order to represent the extreme rainfall- runoff events, the deterministic distributed hydrological modelling is gaining interest both with the increase of the computation facilities and the availability of data especially the topography inputs. Also, in [16] the simulation results of four deterministic hydrological models with different topography resolution (300m,

150m, 75m) for the Var basin, France (2800km2) are analysed with the aim to evaluate the influences on the simulation accuracy. The results of sensitivity analysis indicate the threshold value of the topography resolution on the model simulation with the consideration of both the sufficient accuracy and the reasonable simulation time to cover the extreme rainfall-runoff event in 1994. In [17] the authors introduce a framework for precise vehicle localisation in dense urban environments that are characterised by high rates of dynamic and semi-static objects. The proposed localisation method of [17] is particularly designed for handling the inconsistencies between map material and sensor measurements. The evaluation results of this work show the superior performance of the proposed approach compared to another state-of-the-art localisation algorithm for a challenging urban dataset.

III. TOPOLOGY PROPOSAL

Concerning our research of the Related Research Review section, we developed the following conclusions as a proposal of IoT's contribution in Video Surveillance. A major issue of the Video Surveillance technology is the transmission of data through the video recorder devices and how those devices should be set up with the aim to have a better use of remote control.

As a solution to this problem, we propose an innovative topology paradigm that combines the advantages of the use of IoT and the characteristics of Surveillance. This proposed topology is a hybrid topology of ring and star topologies. In this topology we could succeed a reliable network in error detecting and troubleshooting, we could scalable the size of the network as in can be increased easily, and additionally, this topology offers flexibility and provides a more effective network.

Furthermore, as a combination of two topologies we can operate this network both as a star-topology-network so as a ring-topology-network, as well as a separate type of networks. By using routers with the aim to have single management network sectors, we can achieve a different type of topology use. Figure 1 presents a paradigm of the proposed topology using two types of video surveillance cameras (simple quality surveillance camera and HD quality surveillance camera). The data transmitted from the cameras to the Cloud Server with the useful help of IoT technology and from the Cloud Server transmitted to another local server, and finally we can have all the transmitted data in the storage system of the network server. As it is shown each router could be able to serve a huge number of network cameras, connected to each other with different ways. Also, in this type of network topology, Local Servers can be used inside the small networks as administrators of network cameras. Cloud Server could provide primarily the important role of the storage system, and afterwards could act as data manager that receives these data with the aim to transmit them to the Network Server. Between the Cloud Server and the Network Server, also could interpolate another Local Server in order to clarify and transmit the data to its final destination, which is the Network Server.

An important improvement in the operation of this topology is analysed and described by the following equation:

$$DS = (TD + VD) - PL \quad (1)$$

Equation (1) demonstrates Data send (DS) through the network. This data results by the product of the quantity of the Transmitted data (TD) and the quantity of Video data (VD) deducting the quantity of the Packet Loss (PL). By this equation and regarding the number of nodes existing in the network, we can produce the total amount of data which transmitted through the network. Thus, this calculated by (2):

$$TDS = DS_1 + DS_2 + ... + DS_n \quad (2)$$

Moreover, through our research, we detect that another major issue of the Internet of Things and Video Surveillance technology is the event detection problem in noisy environments for a multimedia monitoring application which is solved with the detection of the abnormality in continuous audio recordings of public places [18]. Regarding the combination of the aforementioned technologies, Table 1 lists the characteristics of the technology of Things, with regard to the convenience it provides. It also demonstrates some of the types of Video Surveillance technology which relates more, in our opinion, to the Internet of Things. Table 1 has the purpose to show which of the specific characteristics of the IoT technology pertain to, and improve the particular types of the Video Surveillance. As we can observe, Cameras and RFID devices are the Video Surveillance types which are affected more by the characteristics of the IoT technology. In contrast, the Biometric is the type of Video Surveillance influenced less by the characteristics of IoT technology.

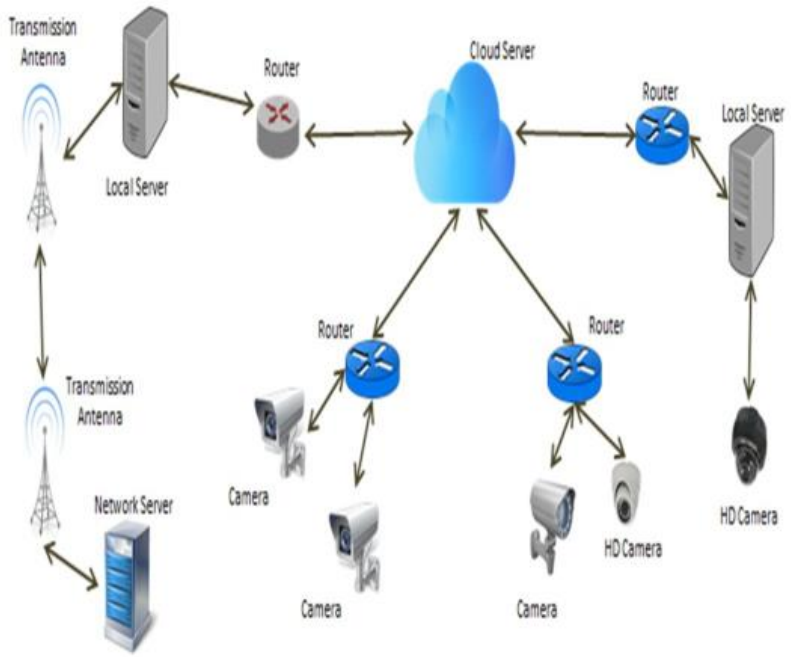


Fig. 1. Proposed topology paradigm.

TABLE I.

Contributions of Internet of Things in Video Surveillance.

Video Surveillance	Computer	Telephones	Cameras	Biometric	Data Mining	RFID
Smart solution in the bucket of transport					X	X
Smart power grids incorporating more renewable	X		X	X		
Remote monitoring of patients	X	X	X	X	X	X
Sensors in homes and airports			X			X
Engine monitoring sensors that detect & predict maintenance issues	X	X	X		X	X

IV. ARCHITECTURE COMPARISON

The study of previous works cites us relevant architecture and topology proposals for a Video Surveillance network, which on several occasions supported and combined with other technologies, such as Internet of Things. In this section we will make a comparative study of the proposal made in this work and proposals made by other relevant works.

On the study conducted we singled out six previous architecture-topology proposals relating to Video Surveillance technology. Here, there will be a comparison between the features and the benefits of each proposal. As we can observe from Table 2 most former works deal with the Quality of Communication, and as the second characteristic that deal with is Security. Thus, the main purpose of these works is to provide secure and quality communication architecture. Comparing our proposed topology to the others we can realise that it contributes more security and privacy issues. It has certainly a disadvantage in relation to the others, as regards the Transmission Speed and the Efficiency.

In addition, the proposed topology of this work could mainly be applied in big buildings, in which there are installed systems of surveillance cameras. Buildings such this could also be defined as Smart Buildings instead of the specialised use of the surveillance system in conjunction with the IoT technology. Thus, the proposed topology can be described as an ideal topology for surveillance systems after using a combination of IoT and Cloud Computing technologies.

TABLE II.

Architectures-Topologies Comparison.

Surveillance Architectures	[20]	[21]	[22]	[23]	[12]	[24]	Proposed
Efficiency		X	X	X		X	
Security		X			X	X	X
Easy Installation	X			X		X	X
Transmission Speed	X	X	X	X			
Quality of Communication	X		X	X	X	X	X
Data Privacy					X		X

V. CONCLUSIONS

With regard to the use of the Video Surveillance and the future needs of this technology, there has been a combination of Video Surveillance technology with Internet of Things technology in order to take advantage of the IoT benefits and improve the use of Video Surveillance. The discussion of this contribution proposes an innovative topology paradigm which could offer a better use of IoT technology in Video Surveillance systems. Also, the contribution of these technologies provided by Internet of Things features in dealing with the basic types of Video Surveillance technology is summarised in Table 1. Additionally, there is a comparison between our proposed topology and relevant proposed topologies focusing on the security issue. Finally, as a future research, we suggest a further examination of the types of Video Surveillance which could be improved from the contribution of the technology of Internet of Things with the additional ‘help' of the Cloud Computing technology.

REFERENCES

[1] Uichin Lee et al, “MobEyes: Smart mobs for urban monitoring with a vehicular sensor network,” IEEE Wireless Communications, pp. 1-15, 1/11/2006.

[2] Dictionary.com, "Dictionary.com", 1/1/2012. [Online]. [Accessed 2/12/2016].

[3] M. Maximino et al, "Journalist's Resourse, Research on today's news topic," 11/2/2014. [Online]. [Accessed 6/3/2016]

[4] J. M. Batalla et al, “Adaptive Video Streaming: Rate and Buffer on the Track of Minimum Rebuffering”, IEEE Journal on Selected Areas in Communications, vol. 34, Issue 8, pp. 2154-2167, 1/8/2016.

[5] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, December 2016.

[6] Sandip Roy et al, "A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework on the Internet of Things," International Journal of Advanced Science and Technology, pp. 23-32, 1/3/2015.

[7] Jordi Mongay Batalla and Piotr Krawiec, "Conception of ID layer performance at the network level for Internet of Things," Pers Ubiquit Comput, no. 18, pp. 465–480, 28/4/2013.

[8] George Kokkonis, Kostas E. Psannis, Manos Roumeliotis, and Yutaka Ishibashi, “Efficient algorithm for transferring a real-time HEVC stream with haptic data through the internet”, Journal of Real-Time Image Processing, May 2015.
[9] George Kokkonis, Kostas E. Psannis, Manos Roumeliotis and Dan Schonfeld, “Real-time wireless multisensory smart surveillance with 3D-HEVC streams for internet-of-things (IoT)”, Journal of Supercompuitng, 2016.
[10] Tiago Cruz et al, “Improving Network Security Monitoring for industrial control systems,” σε Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on, Coimbra, Portugal, 2015.
[11] Daniil Panasetsky et al, "Development of software for modelling decentralized intelligent systems for security monitoring and control in power systems," PowerTech, 2015 IEEE Eindhoven, pp. 1-6, 29/6/2015.
[12] Simone Scardapane et al, "Microphone array based classification for security monitoring in unstructured environments," International Journal of Electronics and Communications (AEÜ), no. 69, pp. 1715-1723, 11/11/2015.
[13] A.C. Mateos & C.M. González, "Physiological response and sulfur accumulation in the biomonitor Ramalina celastri in relation to the concentrations of SO2 and NO2 in urban environments," Microchemical Journal, no. 126, p. 116–123, 1/3/2016.
[14] Jaben Richards et al, "Distribution of pesticides in dust particles in urban environments," Environmental Pollution, no. 214, pp. 290-298, 7/4/2016.
[15] J. Hofman et al, "Ultrafine particles in four European urban environments: Results from a new continuous long-term monitoring network," Atmospheric Environment, no. 136, pp. 68-81, 8/4/2016.
[16] Qiang M.A. et al, "Assessment of High Resolution Topography Impacts on Deterministic Distributed Hydrological Model in Extreme Rainfallrunoff Simulation," in 12th International Conference on Hydroinformatics, HIC 2016, Nice, France, 2016.
[17] Jan Rohde et al, "Precise vehicle localization in dense urban environments," in 19th International IEEE Conference on Intelligent Transportation Systems, Rio de Janeiro, Brazil, 2016.
[18] C. Clavel, T. Ehrette & G. Richard, "Events Detection for an Audio- Based Surveillance System," Multimedia and Expo, 2005. ICME 2005. IEEE International Conference on, pp. 1306-1309, 6/7/2005.
[19] Christos Stergiou & Kostas E. Psannis, "Recent advances delivered by Mobile Cloud Computing and Internet of Things for Big Data applications: a survey," International Journal of Network Management, pp. 1-12, 11/3/2016.
[20] Sola O. Ajiboye et al, "Hierarchical Video Surveillance Architecture - A Chassis for Video Big Data Analytics and Exploration," in Proceedings of SPIE - The International Society for Optical Engineering, Falmer- Brighton, United Kingdom, 2015.
[21] F. Licandro & G. Schembra, "WirelessMesh Networks to Support Video Surveillance: Architecture, Protocol, and Implementation Issues," EURASIP Journal onWireless Communications and Networking, no. 2007, pp. 1-13, 30/1/2007.

[22] S. Dutt & A. Kalra, "A Scalable and Robust Framework for Intelligent Real-time Video Surveillance," Department of Electronics Engineering, Indian Institute Of Technology (BHU), Varanasi, India, 2016.
[23] Henry Detmold et al, "Topology Estimation for Thousand-Camera Surveillance Networks," IEEE, Adelaide, Australia, 2007.
[24] Andreas P. Plageras et al, "IoT-based Surveillance System for Ubiquitous Healthcare," in Industrial Electronics Society , IECON 2016 - 42nd Annual Conference of the IEEE, 22/12/2016.