ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

# IOT SECURITY AND PRIVACY

Διπλωματική Εργασία

του

Στεφάκη Παύλου

Θεσσαλονίκη, Αύγουστος 2021

IOT SECURITY AND PRIVACY

Στεφάκης Παύλος

Πτυχίο Ηλεκτρονικού Μηχανικού ΤΕ, ΑΤΕΙΘ, 2018

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΗΝ ΕΦΑΡΜΟΣΜΕΝΗ ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Ψάννης Κωνσταντίνος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την ηη/μμ/εεεε

| Ονοματεπώνυμο 1 | Ονοματεπώνυμο 2 | Ονοματεπώνυμο 3 |
|---|---|---|
| ..... | ..... | ..... |

Στεφάκης Παύλος

.....

# Περίληψη

Η εποχή του Διαδικτύου των Πραγμάτων (IoT) έχει ήδη ξεκινήσει και θα αλλάξει ριζικά τον τρόπο ζωής μας. Ενώ το IoT μας παρέχει πολλά οφέλη, το IoT μας εκθέτει επίσης σε πολλούς διαφορετικούς τύπους απειλών ασφαλείας στην καθημερινότητά μας. Πριν από το IoT, οι περισσότερες απειλές ασφάλειας σχετίζονταν μόνο με τη διαρροή πληροφοριών και την απώλεια υπηρεσιών. Με το IoT, οι απειλές ασφαλείας μπορούν να επηρεάσουν άμεσα και τον κίνδυνο φυσικής ασφάλειας. Το Διαδίκτυο των Πραγμάτων αποτελείται από διάφορες πλατφόρμες , συσκευές και αισθητήρες με διαφορετικές δυνατότητες και κάθε σύστημα θα χρειαστεί λύσεις ασφαλείας ανάλογα με τα χαρακτηριστικά του. Υπάρχει μεγάλη ζήτηση για λύσεις ασφαλείας που θα μπορούν να υποστηρίζουν πλατφόρμες πολλαπλών προφίλ και να παρέχουν ισοδύναμα επίπεδα ασφαλείας για διάφορες αλληλεπιδράσεις συσκευών. Επιπλέον, η ιδιωτικότητα των χρηστών θα γίνει πιο σημαντική στο περιβάλλον του IoT, επειδή προσωπικές πληροφορίες θα μοιράζονται μεταξύ των συνδεδεμένων πραγμάτων. Γι' αυτό τον λόγο, χρειαζόμαστε μηχανισμούς για την προστασία των προσωπικών δεδομένων και την παρακολούθηση της ροής τους.

**Λέξεις Κλειδιά:** IoT, Ασφάλεια, Ιδιωτικότητα

# Abstract

The era of the Internet of Things (IoT) has already started and it will significally change the way of our lives. While IoT provides us many valuable benefits, it also exposes us to many different types of security threats in our day to day life. Before the arrival of IoT, most security threats were related to information leakage and loss of service. With IoT, security threats can directly influence physical security risk. The Internet of Things consists of various platforms and devices with different capabilities, and each system will need security solutions depending on its characteristics. There is a demand for security solutions that will be able to support multi-profile platforms and provide equivalent security levels for various device interactions. In addition, user privacy will become more important because a lot of personal information will be shared among connected things. Therefore, we need mechanisms to protect personal data and monitor their flow.



**Keywords:** IoT, Security, Privacy

# Περιεχόμενα

# Κατάλογος Εικόνων

# 1 Εισαγωγή

## 1.1 Πρόβλημα – Σημαντικότητα του θέματος

Το IoT θα αποτελείται από δισεκατομμύρια άτομα, μεμονωμένες συσκευές και υπηρεσίες που θα μπορούν να διασυνδέονται μεταξύ τους για να ανταλλάσσουν δεδομένα και χρήσιμες πληροφορίες. Καθώς τα συστήματα IoT θα είναι ευρέως διαδεδομένα, θα προκύψουν πολλά ζητήματα ασφάλειας και ιδιωτικότητας. Αγνοώντας αυτά τα θέματα ασφάλειας και ιδιωτικότητας θα υπάρχουν σοβαρές επιπτώσεις σε διάφορες πτυχές της ζωής μας, όπως τα σπίτια στα οποία ζούμε, τα αυτοκίνητα με τα οποία πηγαίνουμε στη δουλειά μας, ακόμα και τις επιπτώσεις που θα φτάσουν το ίδιο μας το σώμα. Γι' αυτό το λόγο απαιτούνται αξιόπιστες, οικονομικές, αποδοτικές και αποτελεσματικές λύσεις και προστασία της ιδιωτικής ζωής, ώστε να διασφαλίζεται η εμπιστευτικότητα, ακεραιότητα, πιστοποίηση ταυτότητας και ο έλεγχος πρόσβασης, μεταξύ άλλων.

## 1.2 Σκοπός – Στόχοι

Σε αυτή την εργασία, περιγράφονται οι απειλές και οι ανησυχίες για την ασφάλεια και την ιδιωτικότητα που προκύπτουν από τις υπηρεσίες IoT και παρουσιάζονται διάφορες προσεγγίσεις για την επίλυση αυτών των ζητημάτων ασφάλειας και ιδιωτικότητας.

## 1.3 Διάρθρωση της μελέτης

Το 2ο κεφάλαιο της εργασίας εμπεριέχει γενικές πληροφορίες για το IoT καθώς και ένα πλαίσιο αναφοράς που χωρίζει τις λύσεις IoT σε 4 κύρια επίπεδα. Στο 3ο κεφάλαιο συζητάμε για τις προκλήσεις και απαιτήσεις της ασφάλειας του IoT και παρουσιάζουμε την αρχιτεκτονική τριών τομέων. Το 4ο κεφάλαιο αναλύει τις επιθέσεις και τα αντίμετρα για καθένα από τους τρεις τομείς. Τέλος στο επίλογο παρουσιάζονται τα συμπεράσματα καθώς και οι μελλοντικές κατευθύνσεις που πρέπει να ακολουθηθούν ώστε να βελτιωθεί η ασφάλεια και η ιδιωτικότητα του IoT.

# 2 Internet of Things

## 2.1 Τι είναι το IoT ;

Το **Διαδίκτυο των πραγμάτων** ή **Ίντερνετ των πραγμάτων** (**IoT**) είναι το δίκτυο φυσικών αντικειμένων, γνωστών ως "πράγματα", τα οποία είναι ενσωματωμένα με αισθητήρες, λογισμικό και άλλες τεχνολογίες που χρησιμοποιούνται με σκοπό τη σύνδεση και την ανταλλαγή δεδομένων με άλλες συσκευές και συστήματα μεταξύ τους ή και μέσω του Διαδικτύου.[1]

Η έννοια "Things" (πράγματα) δεν είναι αυστηρά συνδεδεμένη με ορισμένα προϊόντα. Αναφέρεται σε μία ευρεία ποικιλία συσκευών εντελώς διαφορετικά μεταξύ τους, όπως για παράδειγμα αυτοκίνητα με ενσωματωμένους αισθητήρες, κλιματιστικά, φωτισμός, κάμερες και συστήματα ασφαλείας, smartwatches κλπ. Βασικό χαρακτηριστικό όλων είναι η σύνδεση μεταξύ τους ή/και στο ίντερνετ.[1]

## 2.2 Ιστορική Αναδρομή

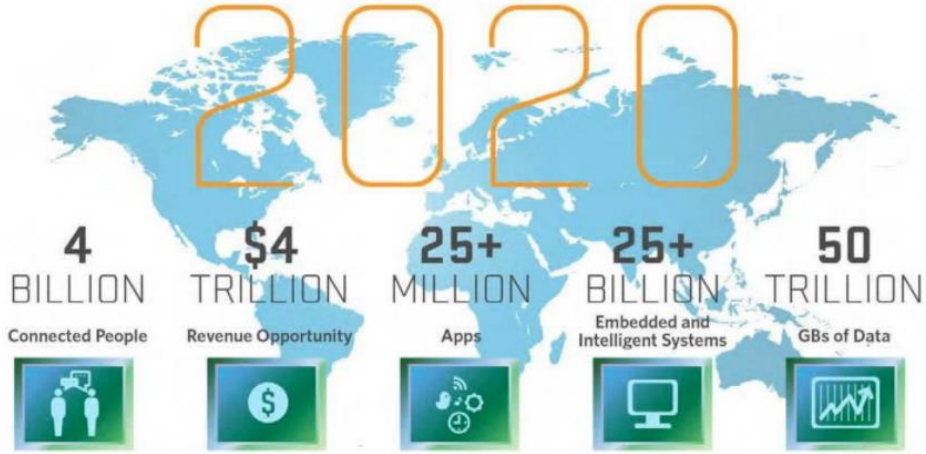
Η κύρια ιδέα ενός δικτύου έξυπνων συσκευών συζητήθηκε ήδη από το 1982, με ένα τροποποιημένο μηχάνημα αυτόματης πώλησης της Coca-Cola στο Πανεπιστήμιο Carnegie Mellon να γίνεται η πρώτη συσκευή που συνδέθηκε με το δίκτυο-ARPANET, ικανή να αναφέρει το απόθεμά της και αν τα πρόσφατα φορτωμένα ποτά ήταν κρύα ή όχι.[2]

Το έγγραφο του Mark Weiser το 1991 "Ο υπολογιστής του 21ου αιώνα", καθώς και ακαδημαϊκοί χώροι όπως το UbiComp και το PerCom παρήγαγαν το σύγχρονο όραμα του IoT. Το 1994, ο Reza Raji περιέγραψε την έννοια στο IEEE Spectrum ως "μετακίνηση μικρών πακέτων δεδομένων σε ένα μεγάλο σύνολο κόμβων, έτσι ώστε να ενσωματωθούν και να αυτοματοποιηθούν τα πάντα, από οικιακές συσκευές μέχρι ολόκληρα εργοστάσια." Μεταξύ 1993 και 1997, διάφορες εταιρείες πρότειναν λύσεις όπως το at Work της Microsoft ή το NEST της Novell. Ο τομέας απέκτησε δυναμική όταν ο Bill Joy οραματίστηκε την επικοινωνία μεταξύ συσκευών ως μέρος του πλαισίου "Six Webs", που παρουσίασε στο Παγκόσμιο Οικονομικό Φόρουμ στο Νταβός το 1999.[2]

Η έννοια του "Διαδικτύου των Πραγμάτων" και ο ίδιος ο όρος, πρωτοεμφανίστηκε σε μια ομιλία του Peter T. Lewis, στο 15ο Ετήσιο Νομοθετικό Σαββατοκύριακο του Congressional Black Caucus Foundation στην Ουάσινγκτον, που δημοσιεύτηκε τον Σεπτέμβριο του 1985. Σύμφωνα με τον Lewis, "Το Διαδίκτυο των Πραγμάτων ή IoT, είναι η ενσωμάτωση ανθρώπων, διαδικασιών και τεχνολογίας με συνδεόμενες συσκευές και αισθητήρες για να καταστεί δυνατή η εξ αποστάσεως παρακολούθηση, η κατάσταση, ο χειρισμός και η αξιολόγηση των τάσεων αυτών των συσκευών".[2]

Ο όρος "Διαδίκτυο των πραγμάτων" επινοήθηκε ανεξάρτητα από τον Kevin Ashton της Procter & Gamble, μετέπειτα Auto-ID Center του MIT, το 1999, αν και ο ίδιος προτιμά τη φράση "Διαδίκτυο για τα πράγματα". Εκείνη τη στιγμή, θεωρούσε την ταυτοποίηση ραδιοσυχνοτήτων (RFID) απαραίτητη για το Διαδίκτυο των πραγμάτων, το οποίο θα επέτρεπε στους υπολογιστές να διαχειρίζονται όλα τα μεμονωμένα πράγματα. Το κύριο θέμα του Διαδικτύου των πραγμάτων είναι η ενσωμάτωση κινητών πομποδεκτών μικρής εμβέλειας σε διάφορα gadgets και είδη καθημερινής ανάγκης, ώστε να επιτρέπονται νέες μορφές επικοινωνίας μεταξύ ανθρώπων και πραγμάτων, αλλά και μεταξύ των ίδιων των πραγμάτων[2]

Ορίζοντας το Διαδίκτυο των Πραγμάτων ως "απλά το χρονικό σημείο κατά το οποίο περισσότερα "πράγματα ή αντικείμενα" συνδέονται στο Διαδίκτυο από ό,τι άνθρωποι", η Cisco Systems εκτιμά ότι το IoT "γεννήθηκε" μεταξύ 2008 και 2009, με την αναλογία πραγμάτων/ανθρώπων να αυξάνεται από 0,08 το 2003 σε 1,84 το 2010.[2]




Εικόνα 2.1 Το IoT το 2020[19]

## 2.3 Γιατί το IoT είναι σημαντικό?

Το IoT βοηθά τους ανθρώπους να ζουν και να εργάζονται πιο έξυπνα, καθώς και να αποκτούν πλήρη έλεγχο της ζωής τους. Εκτός από την προσφορά έξυπνων συσκευών για την αυτοματοποίηση των σπιτιών, το IoT είναι απαραίτητο για τις επιχειρήσεις. Το IoT παρέχει στις επιχειρήσεις μια ματιά σε πραγματικό χρόνο για το πώς λειτουργούν πραγματικά τα συστήματά τους, παρέχοντας πληροφορίες για τα πάντα, από την απόδοση των μηχανών έως τις λειτουργίες της εφοδιαστικής αλυσίδας και των logistics.[3][4]

Το IoT τους επιτρέπει να αυτοματοποιούν τις διαδικασίες και να μειώνουν το κόστος εργασίας. Επίσης, μειώνει τη σπατάλη και βελτιώνει την παροχή υπηρεσιών, καθιστώντας λιγότερο δαπανηρή την κατασκευή και την παράδοση αγαθών, καθώς και προσφέροντας περισσότερη διαφάνεια στις συναλλαγές με τους πελάτες.[3][4]

Ως εκ τούτου, το IoT είναι μια από τις πιο σημαντικές τεχνολογίες της καθημερινής ζωής και θα συνεχίσει να παίρνει φόρα καθώς όλο και περισσότερες επιχειρήσεις συνειδητοποιούν τις δυνατότητες των συνδεδεμένων συσκευών να τις διατηρήσουν ανταγωνιστικές.[3][4]

Ορισμένα παραδείγματα που βρίσκονται στο επίκεντρο είναι [16] :

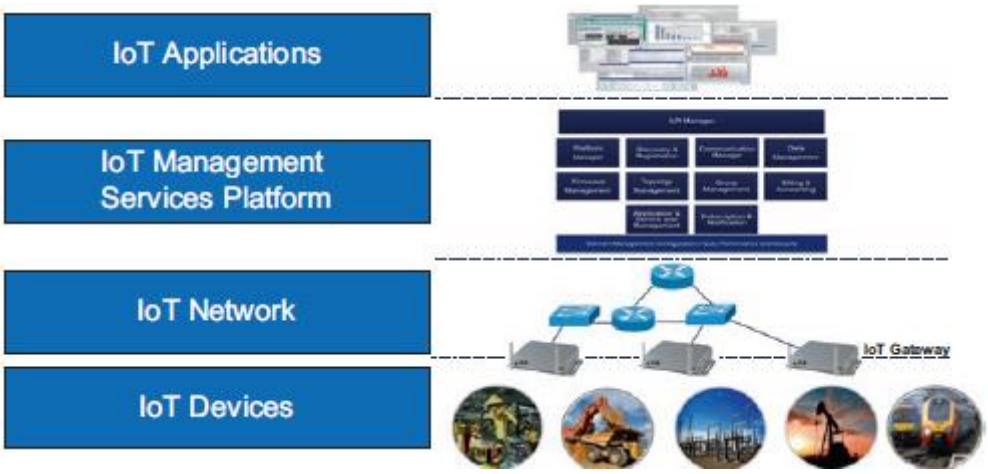
- **Έξυπνη λύση στις μεταφορές** : Με αυτό θα μπορούσαν να επιτευχθούν καλύτερες λύσεις στον τομέα των μεταφορών με στόχο την παροχή ενός καλύτερου τρόπου ζωής.
- **Έξυπνα δίκτυα ηλεκτρικής ενέργειας που ενσωματώνουν περισσότερες ανανεώσιμες πηγές ενέργειας**: Με αυτό θα μπορούσε να επιτευχθεί η αξιοπιστία του συστήματος και επίσης θα μπορούσαν να μειωθούν οι χρεώσεις των καταναλωτών, παρέχοντας έτσι φθηνότερη ηλεκτρική ενέργεια.
- **Απομακρυσμένη παρακολούθηση ασθενών**: Με αυτό θα μπορούσαμε να επιτύχουμε ένα σύστημα που προσφέρει απομακρυσμένη παρακολούθηση των ασθενών. Το σύστημα αυτό θα μπορούσε να προσφέρει ένα καλύτερο και καλά οργανωμένο σύστημα υγειονομικής περίθαλψης, βελτιώνοντας την ποιότητα των υπηρεσιών, αυξάνοντας τον αριθμό των εξυπηρετούμενων ατόμων και εξοικονομώντας χρήματα.

- **Αισθητήρες σε σπίτια, αεροδρόμια και άλλους χώρους:** Με αυτό θα μπορούσαμε να πετύχουμε ασφαλέστερους χώρους, όπως αεροδρόμια και σπίτια, εγκαθιστώντας έναν αριθμό αισθητήρων στο πεδίο.

## 2.4 IoT Reference Framework

Σε αυτή την εργασία ακολουθείτε ένα πλαίσιο αναφοράς που χωρίζει τις λύσεις IoT σε 4 κύρια επίπεδα (εικόνα 2.1) [6] :

- **IoT Device Level** το οποίο αποτελείται από όλες τις συσκευές.
- **IoT Network Level** το οποίο αποτελεί την δομή μεταφοράς δεδομένων και αποτελείται από όλα τα στοιχεία δικτύου (π.χ ρούτερ)
- **IoT Application Services Platform Level** το οποίο περιλαμβάνει το λογισμικό διαχείρισης κύριων λειτουργιών που επιτρέπουν τη συνολική διαχείριση των συσκευών και του δικτύου IoT. Επίσης περιλαμβάνει τις κύριες λειτουργίες που συνδέουν το Device και το Network Level
- **IoT Application Level** το οποίο περιλαμβάνει όλες τις εφαρμογές που λειτουργούν σε ένα δίκτυο IoT**.**




2.2 IoT Reference Framework [6]

Τα κυριότερα πλεονεκτήματα του παραπάνω πλαισίου είναι [6]:

- **Μειωμένη πολυπλοκότητα:** Διαχωρίζει τα στοιχεία και τις διαδικασίες επικοινωνίας του IoT σε μικρότερα και απλούστερα στοιχεία, βοηθώντας έτσι την ανάπτυξη και στο σχεδιασμό τους και την αντιμετώπιση προβλημάτων.
- **Τυποποιημένα στοιχεία και διεπαφές:** το μοντέλο τυποποιεί συγκεκριμένα στοιχεία σε κάθε επίπεδο αλλα και τις διεπαφές μεταξύ των επιπέδων. Αυτό θα επιτρέψει σε διαφορετικούς προμηυθευτές να αναπτύξουν κοινές λύσεις και κοινή υποστήριξη.
- **Μηχανική Ενοτήτων:** επιτρέπει διάφορους τύπους συστημάτων υλικού και λογισμικού IoT να επικοινωνούν μεταξύ τους.
- **Επιτάχυνση της καινοτομίας:** Επιτρέπει στους προγραμματιστές να επικεντρωθούν στην επίλυση του κύριου προβλήματος χωρίς να ανησυχούν για τις βασικές λειτουργίες που μπορούν να υλοποιηθούν μία φορά.

# 3 Ασφάλεια και Ιδιωτικότητα

Στόχος του παρόντος κεφαλαίου είναι να ρίξει φως σε ορισμένα από τα θέματα ασφάλειας και ιδιωτικότητας στα οποία εκτίθεται το IoT. Επίσης, θα δούμε τεχνικές που προτάθηκαν για την αντιμετώπιση αυτών των ζητημάτων. Ορισμένες από τις τεχνικές που συζητήθηκαν αποτρέπουν παραβιάσεις της ασφάλειας από το να λάβουν χώρα, ενώ άλλες προσπαθούν να ανιχνεύσουν κακόβουλη συμπεριφορά και να ενεργοποιήσουν ένα κατάλληλο αντίμετρο.

## 3.1 Προκλήσεις ασφάλειας IoT

Το IoT έχει μοναδικά χαρακτηριστικά και περιορισμούς όσον αφορά τον σχεδιασμό αποτελεσματικών αμυντικών μηχανισμών κατά των απειλών που μπορούν να συνοψιστούν στα εξής [7][21]:

- **Πολλαπλές τεχνολογίες:** Το IoT συνδυάζει πολλές τεχνολογίες, όπως ραδιοσυχνότητες ταυτοποίηση (RFID), ασύρματα δίκτυα αισθητήρων κλπ. Κάθε μία από αυτές τις τεχνολογίες έχει τα δικά της τρωτά σημεία. Το πρόβλημα του IoT είναι ότι πρέπει να διασφαλιστεί η αλυσίδα όλων των αυτών των τεχνολογιών, καθώς η ανθεκτικότητα στην ασφάλεια μιας εφαρμογής IoT θα κριθεί με βάση το πιο αδύναμο σημείο της.
- **Πολλαπλές εφαρμογές:** το IoT θα έχει πολυάριθμες εφαρμογές (πχ. ηλεκτρονική υγεία, τη βιομηχανία, τα έξυπνα οικιακά gadgets κλπ). Οι απαιτήσεις ασφαλείας κάθε εφαρμογής είναι αρκετά διαφορετικές από τις από τις υπόλοιπες.
- **Επεκτασιμότητα:** Ο τεράστιος αριθμός συνδεδεμένων συσκευών καθιστά την επεκτασιμότητα σημαντικό ζήτημα όταν πρόκειται για την ανάπτυξη αποτελεσματικών αμυντικών μηχανισμών. Κανένα από τα προτεινόμενα κεντρικά αμυντικά πλαίσια δεν μπορεί πλέον να λειτουργήσει με το IoT, όπου η εστίαση πρέπει να στραφεί στην εξεύρεση πρακτικών αποκεντρωμένων αμυντικών μηχανισμών ασφαλείας. Μια

λύση IoT πρέπει να κλιμακώνεται οικονομικά αποδοτικά, δυνητικά σε εκατοντάδες χιλιάδες ή και εκατομμύρια τερματικά σημεία.

- **Διαθεσιμότητα:** Η διαθεσιμότητα είναι χαρακτηριστικό ενός συστήματος ή υποσυστήματος που είναι συνεχώς λειτουργικό για ένα επιθυμητά μεγάλο χρονικό διάστημα. Συνήθως μετράτε σε σχέση με το "100% λειτουργικό" ή το "δεν αποτυγχάνει ποτέ". Ένα ευρέως διαδεδομένο αλλά δύσκολο να επιτευχθεί πρότυπο διαθεσιμότητας για ένα σύστημα είναι η γνωστή ως "πέντε 9αρια" (διαθέσιμο 99,999% του χρόνου σε ένα δεδομένο έτος) διαθεσιμότητα. Η Ασφάλεια παίζει σημαντικό ρόλο στην υψηλή διαθεσιμότητα, καθώς οι διαχειριστές δικτύων συχνά διστάζουν να χρησιμοποιούν τις απαραίτητες λειτουργίες της τεχνολογίας αντιμετώπισης απειλών, φοβούμενοι ότι οι λειτουργίες αυτές θα οδηγήσουν σε κατάρρευση του συστήματος. Ακόμα και μια απλή σάρωση πόρτας μπορεί να προκαλέσει τη διακοπή λειτουργίας ορισμένων συσκευών IoT και το κόστος της διακοπής λειτουργίας μπορεί να υπερβαίνει κατά πολύ το κόστος της αποκατάστασης όλων των προβλημάτων εκτός από τα πιο σοβαρά περιστατικά. Σε ορισμένες περιπτώσεις, οι διαχειριστές δικτύων θα προτιμούσαν να μην έχουν προστασία παρά να διακινδυνεύσουν μια διακοπή λειτουργίας λόγω ψευδούς θετικού αποτελέσματος. Αυτό τους αφήνει τυφλούς απέναντι στις απειλές εντός των δικτύων τους. Οι εταιρείες συχνά προσθέτουν πλεονασμό στα συστήματά τους, έτσι ώστε η βλάβη ενός εξαρτήματος να μην επηρεάζει το ολόκληρο το σύστημα.
- **Μεγάλα δεδομένα:** Δεν είναι μόνο ο αριθμός των έξυπνων συσκευών που θα είναι τεράστιος, αλλά και τα δεδομένα που παράγονται από κάθε συσκευή θα είναι τεράστια, καθώς τροφοδοτούνται από πολυάριθμους αισθητήρες, όπου κάθε αισθητήρας παράγει τεράστιες ποσότητες δεδομένων με την πάροδο του χρόνου. Αυτό καθιστά απαραίτητη την εξεύρεση αποτελεσματικών αμυντικών μηχανισμών που μπορούν να ασφαλίσουν αυτές τις μεγάλες ροές δεδομένων.

- **Περιορισμοί πόρων:** Η πλειονότητα των τελικών συσκευών IoT έχουν περιορισμένες δυνατότητες πόρων, όπως CPU, μνήμη, αποθηκευτικό χώρο, μπαταρία και εμβέλεια. Αυτό καθιστά τις εν λόγω συσκευές εύκολο στόχο για επιθέσεις άρνησης παροχής υπηρεσιών (DoS), όπου ο επιτιθέμενος μπορεί εύκολα να εξουδετερώσει τις περιορισμένες δυνατότητες πόρων των εν λόγω συσκευών προκαλώντας διακοπή των υπηρεσιών. Επιπλέον, οι περιορισμένοι πόροι αυτών των συσκευών δημιουργούν νέες προκλήσεις όσον αφορά την ανάπτυξη πρωτοκόλλων ασφαλείας, καθώς οι παραδοσιακές και ώριμες τεχνικές κρυπτογράφησης είναι γνωστό ότι είναι υπολογιστικά δαπανηρές.
- **Απομακρυσμένες τοποθεσίες:** Σε πολλές περιπτώσεις οι συσκευές και οι αισθητήρες πρέπει να εγκατασταθούν σε απομακρυσμένες δύσκολα πρσβάσιμες περιοχές. Οι επιτιθέμενοι μπορούν να παρεμβαίνουν σε αυτές τις συσκευές χωρίς να γίνονται αντιληπτοί. Συστήματα παρακολούθησης της κυβερνοασφάλειας και της φυσικής ασφάλειας πρέπει να εγκατασταθούν σε προστατευμένες τοποθεσίες, να λειτουργούν σε ακραίες περιβαλλοντικές συνθήκες, να χωράνε σε μικρούς χώρους, και να λειτουργούν εξ αποστάσεως για τακτικές ενημερώσεις και συντήρηση αποφεύγοντας καθυστερημένες και δαπανηρές επισκέψεις τεχνικών δικτύου.
- **Κινητικότητα:** Έξυπνες συσκευές αναμένεται να αλλάζουν συχνά τη θέση τους. Αυτό προσθέτει επιπλέον δυσκολίες κατά την ανάπτυξη αποτελεσματικών αμυντικών μηχανισμών σε τέτοια δυναμικά περιβάλλοντα.
- **Υπηρεσία ευαίσθητη στην καθυστέρηση:** Η πλειοψηφία των εφαρμογών IoT είναι ευαίσθητες στην καθυστέρηση, ως εκ τούτου θα πρέπει να προστατεύονται από οποιαδήποτε επίθεση που μπορεί να υποβαθμίσει το χρόνο εξυπηρέτησής τους ή να προκαλέσει μια διακοπή.

## 3.2 Απαιτήσεις ασφάλειας IoT

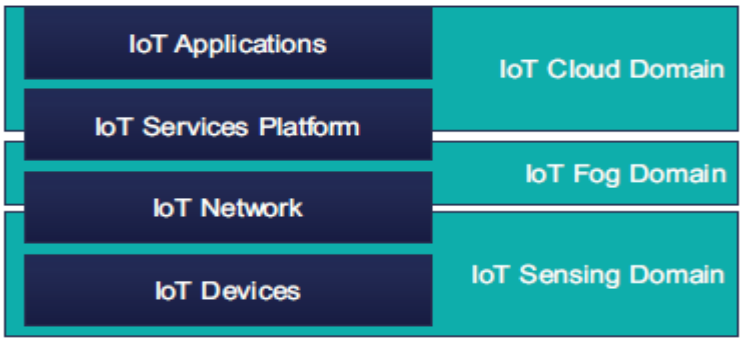
Στην παρούσα ενότητα συνοψίζουμε τις απαιτήσεις ασφάλειας για το IoT. Αυτές οι απαιτήσεις περιλαμβάνουν τα εξής [8][15]:

- **Εμπιστευτικότητα:** διασφαλίζει ότι τα ανταλλασσόμενα μηνύματα μπορούν να γίνουν κατανοητά μόνο από τις προβλεπόμενες οντότητες.
- **Ακεραιότητα:** διασφαλίζει ότι τα ανταλλασσόμενα μηνύματα δεν έχουν αλλοιωθεί/παραποιηθεί.
- **Αυθεντικοποίηση:** διασφαλίζει ότι οι οντότητες που συμμετέχουν σε οποιαδήποτε λειτουργία είναι αυτές που ισχυρίζονται ότι είναι. Μια επίθεση μεταμφίεσης ή μια επίθεση πλαστοπροσωπίας στοχεύει συνήθως σε αυτό το σημείο όπου μια οντότητα ισχυρίζεται ότι είναι μια άλλη.
- **Διαθεσιμότητα:** εξασφαλίζει ότι η υπηρεσία δεν διακόπτεται. Επιθέσεις άρνησης υπηρεσίας στοχεύουν σε αυτό, καθώς προκαλούν διακοπή της υπηρεσίας.
- **Εξουσιοδότηση:** διασφαλίζει ότι οι οντότητες διαθέτουν τα απαιτούμενα δικαιώματα για την εκτέλεση της λειτουργίας που ζητούν να εκτελέσουν
- **Φρεσκάδα:** διασφαλίζει ότι τα δεδομένα είναι φρέσκα. Οι επιθέσεις αναπαραγωγής στοχεύουν αυτό, όπου ένα παλιό μήνυμα αναπαράγεται για να επιστρέψει μια οντότητα σε μια παλιά κατάσταση.
- **Μη άρνηση:** διασφαλίζει ότι μια οντότητα δεν μπορεί να αρνηθεί μια ενέργεια που έχει εκτελέσει.
- **Forward Secrecy:** διασφαλίζει ότι όταν ένα αντικείμενο εγκαταλείπει το δίκτυο, δεν θα κατανοήσει τα μηνύματα που ανταλλάσσονται μετά την αποχώρησή του.
- **Backward Secrecy:** διασφαλίζει ότι οποιοδήποτε νέο αντικείμενο που εισέρχεται στο δίκτυο δεν θα μπορεί να κατανοήσει τα μηνύματα που ανταλλάχθηκαν πριν από την ένταξή του στο δίκτυο.

## 3.3 Αρχιτεκτονική τριών τομέων

Όπως θα δείτε στην παρακάτω εικόνα (εικόνα 3.1) αύτη η αρχιτεκτονική αποτελείται από τους εξής τρείς τομείς [9]:

- **Τομέας Ανίχνευσης(Sensing Domain):** Ο τομέας αυτός αποτελείται από όλα τα έξυπνα αντικείμενα που έχουν τη δυνατότητα να ανιχνεύουν το περιβάλλον και να αναφέρουν τα δεδομένα που ανιχνεύονται σε μία από τις συσκευές του τομέα ομίχλης (Fog Domain). Τα έξυπνα αντικείμενα σε αυτόν τον τομέα αναμένεται να αλλάζουν τη θέση τους με την πάροδο του χρόνου.
- **Τομέας ομίχλης(Fog Domain):** Αυτός ο τομέας αποτελείται από ένα σύνολο συσκευών ομίχλης που βρίσκονται σε περιοχές που είναι ιδιαίτερα πυκνοκατοικημένες από πολλά αντικείμενα. Σε κάθε συσκευή ανατίθεται ένα σύνολο έξυπνων αντικειμένων, τα οποία αναφέρουν τα δεδομένα που έχουν ανιχνευθεί και η συσκευή κάνει την απαιτούμενη επεξεργασία. Οι συσκευές ομίχλης συνδέονται επίσης μεταξύ τους προκειμένου να διαχειρίζονται την επικοινωνία μεταξύ των αντικειμένων και για να συντονίσουν ποια συσκευή θα είναι υπεύθυνη για το χειρισμό ποιου αντικειμένου, καθώς τα αντικείμενα αλλάζουν τη θέση τους με την πάροδο του χρόνου. Κάθε συσκευή ομίχλης συνδέεται επίσης με έναν ή περισσότερους διακομιστές στον τομέα του νέφους(Cloud Domain).
- **Τομέας νέφους(Cloud Domain):** Αυτός ο τομέας αποτελείται από έναν μεγάλο αριθμό διακομιστών που φιλοξενούν τις εφαρμογές που είναι υπεύθυνες για την εκτέλεση των βαρέων υπολογιστικών επεξεργασιών των δεδομένων που αναφέρονται από τις συσκευές ομίχλης.




Εικόνα 3.1 Αρχιτεκτονική τριών τομέων [9]

# 4 Επιθέσεις και Αντίμετρα

Σε αυτή την ενότητα αναλύουμε τις επιθέσεις ασφαλείας και τα αντίμετρα σε κάθε έναν από αυτούς τους προαναφερθέντες τρεις τομείς. Για καθένα από αυτούς τους τομείς, προσδιορίζουμε τις πιο δημοφιλείς επιθέσεις ασφαλείας και ποιες τεχνικές αντιμέτρων μπορούν να χρησιμοποιηθούν. για την πρόληψη, την ανίχνευση ή τον μετριασμό αυτών των επιθέσεων.

## 4.1 Επιθέσεις και Αντίμετρα στον Τομέα νέφους

Κάθε εφαρμογή IoT είναι αφιερωμένη σε μία ή περισσότερες εικονικές μηχανές (VM), όπου κάθε VM έχει ανατεθεί σε έναν από τους διακομιστές στο κέντρο δεδομένων του νέφους και του κατανέμεται ορισμένη ποσότητα πόρων CPU και μνήμης προκειμένου να εκτελεί ορισμένες υπολογιστικές εργασίες. Το υπολογιστικό νέφος αποτελείται από χιλιάδες διακομιστές όπου κάθε διακομιστής διαθέτει ορισμένη CPU, μνήμη και χωρητικότητα αποθήκευσης , επομένως, κάθε διακομιστής έχει ένα όριο στον αριθμό των VM που μπορεί να φιλοξενήσει. Οι διακομιστές στο κέντρο δεδομένων νέφους είναι εικονικοί το οποίο επιτρέπει την ανάθεση πολλαπλών VM στον ίδιο διακομιστή, εφόσον ο διακομιστής έχει αρκετή χωρητικότητα πόρων για να υποστηρίξει τις απαιτήσεις πόρων κάθε φιλοξενούμενου VM. Κάθε εφαρμογή IoT φιλοξενείται σε ένα VM που έχει το δικό του λειτουργικό σύστημα (OS). Ο hypervisor) παρακολουθεί αυτές τις VM και διαχειρίζεται τον τρόπο με τον οποίο αυτές οι VM μοιράζονται το υλικό(Hardware) του διακομιστή. Ο hypervisor παρέχει επίσης τον λογικό διαχωρισμό μεταξύ των VM και διαχωρίζει επίσης κάθε VM από το υλικό(Hardware). Ο hypervisor διαθέτει επίσης μια μονάδα μετανάστευσης που διαχειρίζεται τον τρόπο μετακίνησης ενός VM που φιλοξενείται τώρα στον διακομιστή σε έναν άλλο διακομιστή και τη λήψη ενός VM που είναι μετακινείται από άλλους διακομιστές.

Οι εφαρμογές IoT που εκτελούνται στον τομέα του νέφους είναι ευάλωτες σε πολυάριθμες ασφάλειες επιθέσεις. Μερικές από αυτές είναι οι παρακάτω [10]:

### *4.1.1 Επιθέσεις κρυφού καναλιού (Hidden-Channel Attacks)*

Παρόλο που υπάρχει λογικός διαχωρισμός μεταξύ των VM που εκτελούνται στον ίδιο διακομιστή, εξακολουθούν να υπάρχουν ορισμένα στοιχεία υλικού που μοιράζονται μεταξύ αυτών των VM, όπως η προσωρινή μνήμη cache. Αυτό ανοίγει ευκαιρίες για διαρροή δεδομένων μεταξύ των VM που βρίσκονται στον ίδιο διακομιστή. Τρία βήματα ακολουθούνται από τον επιτιθέμενο προκειμένου να διαρρεύσουν πληροφορίες[10]:

- **1.Χαρτογράφηση του VM-στόχου:** Το πρώτο βήμα προς την έναρξη μιας επίθεσης εναντίον ενός VM σε ένα κέντρο δεδομένων νέφους είναι ο εντοπισμός του τόπου όπου βρίσκεται το VM-στόχος. Ένα κέντρο δεδομένων χωρίζεται συνήθως σε πολλαπλές μονάδες διαχείρισης που ονομάζονται συστάδες, όπου κάθε συστάδα βρίσκεται σε μια συγκεκριμένη γεωγραφική τοποθεσία και αποτελείται από χιλιάδες από διακομιστές. Κάθε συστάδα χωρίζεται σε πολλαπλές ζώνες όπου κάθε ζώνη αποτελείται από μεγάλο αριθμό διακομιστών. Αν και οι πελάτες έχουν την επιλογή να καθορίσουν σε ποια συστάδα βρίσκεται το VM τους, δεν έχουν έλεγχο στην επιλογή της ζώνης ή του διακομιστή εντός της ζώνης όπου το VM τους θα κατοικεί, καθώς η απόφαση αυτή λαμβάνεται με βάση τον αλγόριθμο χρονοπρογραμματισμού του παρόχου νέφους ο οποίος δεν δημοσιοποιείται. Προκειμένου να γνωρίζουμε πού βρίσκεται ένα VM-στόχος, ο επιτιθέμενος χρειάζεται μόνο να γνωρίζει την εξωτερική διεύθυνση IP του εν λόγω VM όπου κάθε VM που φιλοξενείται στο νέφος έχει συνήθως δύο διευθύνσεις IP: μια εξωτερική διεύθυνση που χρησιμοποιείται για την επικοινωνία με οποιαδήποτε οντότητα που βρίσκεται εκτός της συστάδας του νέφους και μια εσωτερική διεύθυνση που χρησιμοποιείται μόνο εντός της συστάδας υπολογιστικού νέφους και είναι ορατή μόνο εντός της συστάδας. Ο επιτιθέμενος μπορεί να συμπεράνει με βάση την εξωτερική διεύθυνση IP του VM στο ποια συστάδα βρίσκεται το VM, καθώς οι συστάδες τοποθετούνται όπως είπαμε συνήθως σε διαφορετικές γεωγραφικές τοποθεσίες και έχουν διαφορετικές διευθύνσεις IP. Τώρα, προκειμένου να εντοπίσει σε ποια ζώνη εντός της συστάδας βρίσκεται το VM-στόχος, ο επιτιθέμενος πρέπει να γνωρίζει την εσωτερική διεύθυνση IP του VM-στόχου, καθώς οι εσωτερικές διευθύνσεις IP για όλα τα VM εντός του της

ίδιας ζώνης έχουν το ίδιο πρόθεμα δικτύου. Προκειμένου να προσδιοριστεί η εσωτερική διεύθυνση του VM-στόχου διεύθυνση IP, ο επιτιθέμενος νοικιάζει ένα VM στην ίδια συστάδα με αυτή στην οποία βρίσκεται ο στόχος. Στη συνέχεια, το νοικιασμένο VM χρησιμοποιείται για να ζητήσει από τον διακομιστή DNS του νέφους από τον οποίο μπορεί να αντληθεί η εσωτερική διεύθυνση IP του VM-στόχου. Παρατηρώντας την εσωτερική διεύθυνση IP του VM-στόχου στο ερώτημα DNS, ο επιτιθέμενος μπορεί να καταλάβει σε ποια ζώνη εντός της συστάδας φιλοξενείται το VM.

- **2.Κακόβουλη τοποθέτηση VM:** έχοντας εντοπίσει σε ποια συστάδα και σε ποια ζώνη βρίσκεται το VM-στόχος, το επόμενο βήμα είναι η τοποθέτηση ενός κακόβουλου VM στον ίδιο διακομιστή όπου βρίσκεται το VM-στόχος. Για να γίνει αυτό, ο επιτιθέμενος νοικιάζει ένα VM στην ίδια συστάδα με τον VM-στόχου. Ο αλγόριθμος χρονοπρογραμματισμού του παρόχου τοποθετεί το νοικιασμένο VM στον έναν από τους διακομιστές σε μία από τις ζώνες της συστάδας. Ο επιτιθέμενος εκτελεί ένα traceroute από το νοικιασμένο VM στο VM-στόχο, όπου το μονοπάτι δρομολόγησης που χωρίζει το νοικιασμένο VM και το VM-στόχο εντοπίζεται. Εάν το αναγνωρισμένο μονοπάτι δρομολόγησης δείχνει πολλαπλά άλματα που χωρίζουν το VM-στόχο και το νοικιασμένο VM, τότε ο επιτιθέμενος γνωρίζει ότι το νοικιασμένο VM δεν τοποθετήθηκε στον ίδιο διακομιστή με τον στόχο VM. Στη συνέχεια, ο επιτιθέμενος απελευθερώνει το νοικιασμένο VM και ζητά ένα νέο. Η ίδια διαδικασία επαναλαμβάνετε μέχρι ο επιτιθέμενος να διαπιστώσει ότι ο αλγόριθμος έχει τοποθετήσει το νοικιασμένο VM στον ίδιο διακομιστή με το VM-στόχο.
- **3.Διαρροή δεδομένων μεταξύ των VM:** Έχοντας τοποθετήσει ένα κακόβουλο VM στον ίδιο διακομιστή με το VM-στόχο, ο επιτιθέμενος προσπαθεί τώρα να μάθει κάποιες πληροφορίες σχετικά με το VM-στόχο, εκμεταλλευόμενος το γεγονός ότι αν και τα VM είναι λογικά διαχωρισμένα, εξακολουθούν να μοιράζονται ορισμένα τμήματα του υλικού του διακομιστή όπως η κρυφή μνήμη εντολών και η κρυφή μνήμη δεδομένων. Ο επιτιθέμενος μπορεί τώρα, για παράδειγμα, να μάθει σε

ποιες γραμμές της κρυφής μνήμης έχει προσπελάσει το VM-στόχος πρόσφατα. Γνωρίζοντας ποιες διευθύνσεις προσπελαύνει το VM-στόχος με την πάροδο του χρόνου μπορεί να βοηθήσει το κακόβουλο VM να ανακτήσει τμήματα των κλειδιών ασφαλείας που χρησιμοποιεί το VM-στόχος.

Μπορούν να ληφθούν διάφορα αντίμετρα για την αποτροπή επιθέσεων κρυφού καναλιού από να λάβει χώρα. Τα πρώτα δύο βήματα που απαιτούνται για την πραγματοποίηση αυτής της επίθεσης μπορούν να αποτραπούν με το να μην επιτρέπεται στα VM που φιλοξενούνται στο κέντρο δεδομένων να στέλνουν ανιχνευτικά πακέτα, όπως πακέτα traceroute. Αποτροπή της διαρροής δεδομένων σε VM που φιλοξενούνται στον ίδιο διακομιστή μπορεί να επιτευχθεί με ένα από τα ακόλουθα τεχνικές [9]:

- **Σκληρή απομόνωση:** Η βασική ιδέα πίσω από αυτή την προληπτική τεχνική είναι η διατήρηση υψηλών επιπέδων απομόνωσης μεταξύ των VM. Αυτό γίνεται με διάφορους τρόπους. Ένας από τους καλύτερους τρόπους για την επίτευξη σκληρής απομόνωσης είναι αφήνοντας κάθε πελάτη να καθορίσει έναν κατάλογο αξιόπιστων υπηρεσιών νέφους που ονομάζεται λευκή λίστα. Ο πελάτης δεν έχει πρόβλημα να μοιράζεται τον διακομιστή μόνο με τα VM που ανήκουν στους χρήστες της λευκής λίστας. Νέοι αλγόριθμοι χρονοπρογραμματισμού απαιτούνται σε αυτή την περίπτωση προκειμένου να αποφασιστεί σε ποιον διακομιστή θα πρέπει να τοποθετηθεί κάθε VM έτσι ώστε οι περιορισμοί ασφαλείας κάθε VM που καθορίζονται από τους λευκές και μαύρες λίστες να τηρούνται. Ένας βασικός περιορισμός αυτής της τεχνικής είναι ότι κάθε VM πρέπει να έχει έναν κατάλογο αναγνωρισμένων αναξιόπιστων VM.
- **Εκκαθάριση κρυφής μνήμης:** Αυτή η τεχνική εκκαθαρίζει την κοινόχρηστη κρυφή μνήμη κάθε φορά που η κατανομή της κρυφής μνήμης αλλάζει από ένα VM σε ένα άλλο. Το μειονέκτημα αυτού του αντιμέτρου είναι ότι τα VM που εκτελούνται στο διακομιστή θα παρουσιάζουν συχνή υποβάθμιση επιδόσεων, καθώς η κοινόχρηστη κρυφή μνήμη θα αδειάζει κάθε φορά που γίνεται εναλλαγή από ένα VM σε άλλο, γεγονός που αυξάνει το χρόνο που απαιτείται για την πρόσβαση και την άντληση δεδομένων.

- **Χρόνος πρόσβασης σε δεδομένα με θόρυβο:** Αυτή η τεχνική προσθέτει τυχαίο θόρυβο στην ποσότητα των χρόνο που απαιτείται για την άντληση δεδομένων, γεγονός που καθιστά δύσκολο να διαπιστωθεί αν τα δεδομένα ήταν ή όχι από την κρυφή μνήμη ή από τη μνήμη. Με τον τρόπο αυτό, γίνεται πιο δύσκολο για ένα κακόβουλο VM να εντοπίσει ποια τμήματα της κρυφής μνήμης συμπληρώθηκαν από ένα άλλο VM που μοιράζεται τον ίδιο διακομιστή. Φυσικά αυτό έχει ένα τίμημα, καθώς τα ανακτηθέντα δεδομένα καθυστερούν λίγο λόγω του θορύβου που προστίθεται στο χρόνο που απαιτείται για την ανάκτηση των δεδομένων.
- **Περιορισμός του ρυθμού εναλλαγής της κρυφής μνήμης**: Μια τεχνική μετριασμού για τον περιορισμό της ποσότητας δεδομένων που μπορούν να διαρρεύσουν μεταξύ των VM μπορεί να επιτευχθεί με τον περιορισμό της συχνότητας με την οποία η προσωρινή μνήμη αλλάζει από ένα VM σε ένα άλλο. Η ιδέα εδώ είναι ότι εάν η κρυφή μνήμη δεν αλλάζει από ένα VM σε ένα άλλο πολύ σύντομα, τότε το περιεχόμενο της κρυφής μνήμης θα έχει τροποποιηθεί πολύ από το VM που κατέχει την κρυφή μνήμη. Αυτό καθιστά δύσκολο για ένα κακόβουλο-VM να αποκτήσει λεπτομερή γνώση των δεδομένων στα οποία είχε πρόσβαση το προηγούμενο VM όταν εξετάζει την κρυφή μνήμη.

### *4.1.2 Επιθέσεις μετανάστευσης VM*

Η τεχνολογία εικονικοποίησης υποστηρίζει ζωντανή μετανάστευση VM, η οποία επιτρέπει τη διαφανή μετακίνηση ενός VM από έναν διακομιστή σε έναν άλλο. Ο όρος ζωντανή αναφέρεται εδώ στο γεγονός ότι η εφαρμογή που εκτελείται στο VM διακόπτεται για πολύ σύντομο χρονικό διάστημα λόγω αυτής της μετανάστευσης, όπου η διαταραχή είναι τόσο μικρή όσο εκατοντάδες χιλιοστά του δευτερολέπτου. Οι ανέσεις που φέρνει η μετανάστευση VM εγείρουν νέες απειλές για την ασφάλεια. Οι επιθέσεις που εκμεταλλεύονται τις VM μετανάστευσης μπορούν να χωριστούν σε δύο υποκατηγορίες με βάση το επίπεδο-στόχο.[10]

#### *4.1.2.1 Επιθέσεις στο επίπεδο ελέγχου*

Αυτές οι επιθέσεις στοχεύουν τη μονάδα που είναι υπεύθυνη για το χειρισμό τη διαδικασία μετάβασης σε έναν διακομιστή, η οποία ονομάζεται μονάδα μετάβασης και βρίσκεται στον hypervisor. Με την εκμετάλλευση ενός σφάλματος στο λογισμικό της μονάδας μετανάστευσης, ο επιτιθέμενος μπορεί να παραβιάσει τον διακομιστή και να αναλάβει τον πλήρη έλεγχο της μονάδας μετανάστευσης.

Αυτό δίνει στον επιτιθέμενο τη δυνατότητα να ξεκινήσει κακόβουλες δραστηριότητες, όπως[10]:

- **Πλημμυρισμός Μετανάστευσης:** όπου ο επιτιθέμενος μετακινεί όλα τα VM που φιλοξενούνται στον παραβιασμένο διακομιστή σε έναν διακομιστή-θύμα που δεν έχει αρκετή χωρητικότητα πόρων για να φιλοξενήσει όλα τα μετακινούμενα VM. Αυτή η προκαλεί άρνηση εξυπηρέτησης των εφαρμογών που εκτελούνται στα VM του θύματος-διακομιστή, καθώς δεν θα υπάρχουν αρκετοί πόροι για να ικανοποιήσουν τις απαιτήσεις όλων των VM που φιλοξενούνται με αποτέλεσμα την υποβάθμιση των επιδόσεων των VM και τις καταρρεύσεις των VM.
- **Ψευδής διαφήμιση πόρων:** Ο χακαρισμένος διακομιστής ισχυρίζεται ότι έχει μια μεγάλη ποσότητα ελεύθερων πόρων. Αυτό προσελκύει άλλους διακομιστές να εκφορτώσουν κάποια από τα VM τους στον χακαρισμένο διακομιστή, ώστε ο φόρτος εργασίας του νέφους να κατανέμεται στους διακομιστές. Μετά τη μετακίνηση των VM από άλλους διακομιστές στον παραβιασμένο διακομιστή, ο εισβολέας μπορεί να εκμεταλλευτεί άλλες ευπάθειες για να εισέλθει στα VM, καθώς τώρα αυτά τα VM τοποθετούνται σε έναν διακομιστή που βρίσκεται κάτω από τον έλεγχο του επιτιθέμενου.

#### *4.1.2.2 Επιθέσεις στο επίπεδο δεδομένων*

Οι επιθέσεις αυτές αποτελούν τον δεύτερο τύπο επιθέσεων μετανάστευσης VM, και οι επιθέσεις αυτές στοχεύουν στις συνδέσεις δικτύου μέσω των οποίων μετακινείται το VM από ένα διακομιστή σε άλλον. Παραδείγματα επιθέσεων στο επίπεδο δεδομένων περιλαμβάνουν[10]:

- **Επίθεση Sniffing:** όπου ένας εισβολέας παρακολουθεί τα πακέτα που ανταλλάσσονται μεταξύ της πηγής και του προορισμού και διαβάζει τις μεταφερόμενες σελίδες μνήμης.

- **Επίθεση Man-in-the-Middle:** Ο επιτιθέμενος κατασκευάζει μια απάντηση-πακέτο παρόμοια με αυτό που συνήθως αποστέλλεται όταν ένα VM μετακινείται από ένα διακομιστή σε άλλον. Αυτό το κατασκευασμένο πακέτο ενημερώνει τις συσκευές δρομολόγησης ότι η φυσική διεύθυνση στην οποία βρίσκεται το VM του θύματος άλλαξε και έγινε η φυσική διεύθυνση του κακόβουλου VM του επιτιθέμενου. Τώρα τα εισερχόμενα πακέτα που προορίζονται για το θύμα δρομολογούνται στη νέα φυσική διεύθυνση όπου βρίσκεται ο επιτιθέμενος.

Για την ασφαλή μετανάστευση VM, αμοιβαία αυθεντικοποίηση θα πρέπει να πραγματοποιείται μεταξύ του διακομιστή που ξεκινά τη μετάβαση και του διακομιστή που θα φιλοξενήσει το μεταφερόμενο VM. Τα μηνύματα ελέγχου που ανταλλάσσονται μεταξύ των διακομιστών για τη διαχείριση της μετανάστευσης θα πρέπει επίσης να κρυπτογραφούνται και να είναι υπογεγραμμένα από την οντότητα που παράγει αυτά τα μηνύματα ελέγχου, προκειμένου να αποφευχθεί η αλλοίωση του περιεχομένου αυτών των μηνυμάτων ελέγχου και προκειμένου να αποτραπούν άλλες οντότητες από την κατασκευή πλαστών μηνυμάτων ελέγχου. Οι αύξοντες αριθμοί ή οι χρονοσφραγίδες θα πρέπει να περιλαμβάνονται επίσης στα ανταλλασσόμενα μηνύματα ελέγχου, ώστε να αποτρέπεται η κακόβουλη οντότητα να αναπαράγει ένα παλιό μήνυμα ελέγχου που είχε σταλεί νωρίτερα. Επίσης, τα πακέτα που ενημερώνουν τη φυσική διεύθυνση του VM θα πρέπει να γίνονται δεκτά μόνο μετά από έλεγχο ταυτότητας, προκειμένου να αποτραπούν επιθέσεις man-in-the-middle.[10]

### *4.1.3 Επίθεση κλοπής υπηρεσιών*

Με αυτή την επίθεση ένα κακόβουλο VM συμπεριφέρεται με τρόπο που κάνει τον hypervisor να του αναθέτει περισσότερους πόρους από το μερίδιο που υποτίθεται ότι μπορεί να λάβει. Αυτή η επιπλέον κατανομή πόρων για το κακόβουλο VM έρχεται σε εις βάρος των άλλων VM που μοιράζονται τον ίδιο διακομιστή με το κακόβουλο VM, όπου αυτά τα VM-θύματα λαμβάνουν μικρότερο μερίδιο πόρων από αυτό που θα έπρεπε να λαμβάνουν στην πραγματικότητα, γεγονός που με τη σειρά του υποβαθμίζει την απόδοσή τους. Ένας από τους κύριους ρόλους του hypervisor είναι να αποφασίζει σε ποια VM από τις VM που εκτελούνται στο διακομιστή θα πρέπει να ανατεθεί κάθε φυσικός πυρήνας με την πάροδο του χρόνου. Για να γίνει αυτό, ο hypervisor λαμβάνει δείγματα κάθε 10 χιλιοστά του δευτερολέπτου για να ελέγχει τα VM που χρησιμοποιούν τους πυρήνες. Στη συνέχεια υποθέτει ότι το VM που εντοπίζεται να χρησιμοποιεί έναν από τους πυρήνες κατά τη δειγματοληψία χρησιμοποιεί τον πυρήνα του διακομιστή καθ' όλη τη διάρκεια των 10 χιλιοστών του δευτερολέπτου. Στη συνέχεια, ο hypervisor υπολογίζει πόσος χρόνος έχει ανατεθεί στους πυρήνες σε κάθε VM. Στα VM που χρησιμοποίησαν τους πυρήνες λιγότερο από τα υπόλοιπα VM δίνεται υψηλότερη προτεραιότητα για την χρήση του πυρήνα του διακομιστή στο μέλλον, προκειμένου να διασφαλιστεί η δίκαιη κατανομή των κοινόχρηστων πόρων. [10]

Για την αντιμετώπιση αυτής της επίθεσης προτάθηκαν δύο αντίμετρα. Το πρώτο αντίμετρο είναι η ακριβέστερη καταγραφή της ώρας έναρξης και λήξης όταν κάθε VM χρησιμοποιεί τους πυρήνες χρησιμοποιώντας ακριβή ρολόγια. Μια άλλη λύση είναι η τυχαιοποίηση των χρόνων δειγματοληψίας.[10]

### *4.1.4 Επίθεση διαφυγής VM*

Οι εικονικές μηχανές είναι σχεδιασμένες με τρόπο που απομονώνουν κάθε VM από τις άλλες VM που εκτελούνται στον ίδιο διακομιστή, γεγονός που αποτρέπει τις VM από το να έχουν πρόσβαση σε δεδομένα που ανήκουν σε άλλα VM που βρίσκονται στον ίδιο διακομιστή. Ωστόσο, στην πραγματικότητα μπορούν να αξιοποιηθούν σφάλματα λογισμικού για να σπάσει αυτή η απομόνωση. Εάν ένα VM ξεφύγει από το επίπεδο hypervisor και φτάσει στο υλικό του διακομιστή, τότε το κακόβουλο VM μπορεί να αποκτήσει πρόσβαση root σε ολόκληρο τον διακομιστή όπου βρίσκεται. Αυτό δίνει στο VM πλήρη έλεγχο σε όλα τα VM που φιλοξενούνται στον παραβιασμένο διακομιστή.[10]

Διαφορετικές τεχνικές προτάθηκαν για να αποτραπεί η παράκαμψη του hypervisor από ένα κακόβουλο VM. και να αποκτήσει τα δικαιώματα root. Ένα παράδειγμα τέτοιων τεχνικών είναι το CloudVisor που ουσιαστικά προσθέτει ένα επιπλέον στρώμα απομόνωσης μεταξύ του υλικού και του hypervisor[10]

### *4.1.5 Επιθέσεις εκ των έσω*

Σε όλες τις επιθέσεις που συζητήθηκαν προηγουμένως, αντιμετωπίζαμε τους διαχειριστές του κέντρου δεδομένων νέφους ως έμπιστες οντότητες και εστιάζαμε μόνο στις επιθέσεις που προέρχονται από άλλα κακόβουλα VM που φιλοξενούνται στο κέντρο δεδομένων νέφους. Ωστόσο, ορισμένες ευαίσθητες εφαρμογές μπορεί να έχουν σοβαρές ανησυχίες σχετικά με τη φιλοξενία των συλλεγόμενων πληροφοριών τους στο νέφος δεδομένων καθώς οι διαχειριστές του κέντρου δεδομένων υπολογιστικού νέφους σε αυτή την περίπτωση θα έχουν τη δυνατότητα πρόσβασης και τροποποίησης των συλλεγόμενων δεδομένων. Διαφορετικές τεχνικές προτάθηκαν για την προστασία των δεδομένων από αυτές τις εσωτερικές επιθέσεις. Η Ομομορφική κρυπτογράφηση είναι μια μορφή κρυπτογράφησης που μπορεί να χρησιμοποιηθεί για την αποτροπή τέτοιων επιθέσεων, καθώς επιτρέπει στους διακομιστές νέφους να εκτελούν ορισμένες υπολογιστικές λειτουργίες σε κρυπτογραφημένα δεδομένα εισόδου για τη δημιουργία ενός κρυπτογραφημένου αποτελέσματος.

Αυτό το κρυπτογραφημένο αποτέλεσμα όταν αποκρυπτογραφείται ταιριάζει με το αποτέλεσμα της εκτέλεσης της υπολογιστικής πράξης στα μη κρυπτογραφημένα δεδομένα εισόδου.[10]

| Attack | Vulnerability reason | Security violation | Countermeasures |
|---|---|---|---|
| Hidden-channel attack | Shared hardware components (e.g., cache) among the server's VMs | Confidentiality | Hard isolation<br>Cache flushing<br>Noisy data access time<br>Limiting cache switching rate |
| VM migration attacks | VM migration software bugs<br>VM migration is performed without authentication<br>Memory pages copied in clear | Confidentiality<br>Integrity<br>Availability | Server authentication<br>Encrypting migrated memory pages |
| Theft-of-service attack | Periodic sampling of VMs' used resources | Availability<br>Non-repudiation | Fine-grain sampling using high precision clocks<br>Random sampling |
| VM escape attack | Hypervisor software bugs | Confidentiality<br>Availability<br>Integrity | Add an isolation domain between the hypervisor and hardware |
| Insider attacks | Lack of trust in cloud administrators | Confidentiality<br>Integrity | Homomorphic encryption<br>Secret storage through data chopping and permutation based on a secret key |

Εικόνα 4.1 Επιθέσεις και Αντίμετρα στον Τομέα νέφους[10]

## 4.2 Επιθέσεις και αντίμετρα στον τομέα της ομίχλης

Υπενθυμίζεται ότι ο τομέας ομίχλης αποτελείται από ένα σύνολο συσκευών ομίχλης, όπου κάθε συσκευή ομίχλης συλλέγει τα δεδομένα ανίχνευσης που αναφέρονται από ένα σύνολο έξυπνων αντικειμένων. Η συσκευή ομίχλης εκτελεί διάφορες λειτουργίες στα δεδομένα που συλλέγονται, οι οποίες περιλαμβάνουν τη συγκέντρωση δεδομένων, την προεπεξεργασία δεδομένων και την αποθήκευση δεδομένων. Η συσκευή ομίχλης μπορεί επίσης να εκτελεί κάποια συλλογιστική πράξεις στα συλλεχθέντα δεδομένα. Μετά την επεξεργασία και τη συγκέντρωση των συλλεχθέντων δεδομένων, η συσκευή ομίχλης προωθεί αυτά τα δεδομένα στον τομέα νέφους. Οι μεγάλες ομοιότητες μεταξύ του πεδίου της ομίχλης και του τομέα του νέφους καθιστούν τον τομέα της ομίχλης ευάλωτο σε όλες τις επιθέσεις του τομέα του νέφους που περιεγράφηκαν παραπάνω.

Παρόλο που ο τομέας της ομίχλης μοιάζει σε μεγάλο βαθμό με τον τομέα του νέφους, υπάρχουν τρεις βασικές διαφορές που διακρίνουν τις συσκευές ομίχλης από τους διακομιστές νέφους[11]:

- **Τοποθεσία:** Σε αντίθεση με τους διακομιστές νέφους που συνήθως βρίσκονται μακριά από τα έξυπνα αντικείμενα, οι συσκευές ομίχλης τοποθετούνται σε περιοχές με υψηλή πρόσβαση και έτσι τοποθετούνται κοντά στα έξυπνα αντικείμενα. Αυτό παίζει σημαντικό ρόλο στο να δοθεί στις συσκευές ομίχλης η δυνατότητα να ανταποκρίνονται γρήγορα στις αλλαγές των δεδομένων. Αυτό δίνει επίσης στις συσκευές ομίχλης τη δυνατότητα να παρέχουν υπηρεσίες με επίγνωση της τοποθεσίας αφού τα έξυπνα αντικείμενα συνδέονται με την πλησιέστερη συσκευή ομίχλης και έτσι κάθε συσκευή ομίχλης γνωρίζει την θέση των αντικειμένων που συνδέονται με αυτήν.
- **Κινητικότητα:** Δεδομένου ότι η θέση του έξυπνου αντικειμένου μπορεί να αλλάξει με την πάροδο του χρόνου, τότε τα VM που έχουν δημιουργηθεί για να χειρίζονται αυτά τα αντικείμενα στον τομέα ομίχλης πρέπει να μετακινηθούν από μια συσκευή ομίχλης συσκευή σε μια άλλη, προκειμένου να διατηρηθεί η επεξεργασία που εκτελείται στην συσκευή ομίχλης κοντά στο αντικείμενο που παράγει δεδομένα.
- **Χαμηλότερη υπολογιστική ικανότητα**: Οι συσκευές ομίχλης που είναι εγκατεστημένες σε μια συγκεκριμένη τοποθεσία έχουν χαμηλότερη υπολογιστική ικανότητα σε σύγκριση με τις ικανότητες που προσφέρουν τα κέντρα δεδομένων νέφους, καθώς τα τελευταία αποτελούνται από χιλιάδες διακομιστές.

Τα χαρακτηριστικά αυτά εγείρουν νέες απειλές για την ασφάλεια που αφορούν ειδικά τον τομέα της ομίχλης και τον διακρίνουν από τον τομέα του νέφους. Οι απειλές ασφάλειας που είναι ειδικές στον τομέα της ομίχλης είναι οι εξής[11]:

- **Ζητήματα αυθεντικοποίησης και εμπιστοσύνης:** Το γεγονός ότι οι συσκευές ομίχλης δεν απαιτούν ένα μεγάλο χώρο εγκαταστάσεων ή μεγάλο αριθμό διακομιστών σε σύγκριση με τα κέντρα δεδομένων νέφους θα ενθαρρύνει πολλές μικρές και λιγότερο γνωστές εταιρείες να εγκαταστήσουν εικονικές συσκευές ομίχλης σε πυκνοκατοικημένες περιοχές και να προσφέρουν αυτούς τους υπολογιστικούς πόρους προς ενοικίαση από τα έξυπνα αντικείμενα που βρίσκονται κοντά στις εγκατεστημένες συσκευές ομίχλης. Σε αντίθεση με τα κέντρα δεδομένων νέφους τα οποία προσφέρονται από γνωστές εταιρείες, οι συσκευές ομίχλης αναμένεται να είναι ανήκουν σε πολλαπλές και λιγότερο γνωστές οντότητες. Μια σημαντική ανησυχία για την ασφάλεια που πρέπει να λαμβάνεται υπόψη κατά την ανάθεση ενός έξυπνου αντικειμένου σε μια συσκευή ομίχλης είναι να πιστοποιηθεί πρώτα η ταυτότητα του ιδιοκτήτη της συσκευής ομίχλης. Η Αυθεντικοποίηση δεν αρκεί, καθώς το έξυπνο αντικείμενο πρέπει επίσης να αποφασίσει αν ο ιδιοκτήτης της συσκευής ομίχλης είναι αξιόπιστος Τα συστήματα φήμης, είναι μια καλή λύση για την κατάταξη των παρόχων νέφους μπορούν να χρησιμοποιηθούν για να επιλεγεί μια αξιόπιστη συσκευή ομίχλης μεταξύ των διαθέσιμων στην περιοχή που περιβάλλει κάθε έξυπνο αντικείμενο.

- **Υψηλότεροι κίνδυνοι ασφάλειας της μετανάστευσης:** Παρόλο που η μετανάστευση VM είναι κοινή τόσο στη νέφους όσο και στους τομείς της ομίχλης, υπάρχει μια σημαντική διαφορά μεταξύ τους. Ενώ τα μεταναστευμένα VM στο τομέα νέφους μεταφέρονται μέσω του εσωτερικού δικτύου του κέντρου δεδομένων νέφους, οι μεταναστεύσεις από μια συσκευή ομίχλης σε μια άλλη μεταφέρονται μέσω του διαδικτύου. Έτσι, υπάρχει μεγαλύτερη πιθανότητα τα μετακινούμενα VM να εκτεθούν σε εκτεθειμένα συνδέσεις δικτύου ή δρομολογητές δικτύου κατά τη μετακίνηση ενός VM από μια συσκευή fog σε άλλη Αυτό καθιστά ζωτικής σημασίας την κρυπτογράφηση του μετακινούμενου VM και την αυθεντικοποίηση των μηνυμάτων μετανάστευσης VM που ανταλλάσσονται μεταξύ των συσκευών ομίχλης.

- **Υψηλότερη ευπάθεια σε επιθέσεις DoS:** Δεδομένου ότι οι συσκευές ομίχλης έχουν χαμηλότερη υπολογιστική ικανότητα, αυτό τις καθιστά ιδανικές για επιθέσεις άρνησης παροχής υπηρεσιών (DoS) όπου οι επιτιθέμενοι μπορούν εύκολότερα να κυριεύσουν τις συσκευές ομίχλης σε σύγκριση με τις κέντρα δεδομένων νέφους.

- **Πρόσθετες απειλές για την ασφάλεια λόγω της χρήσης εμπορευματοκιβωτίων:** Προκειμένου να παρέχονται οι υπολογιστικές ανάγκες για μεγαλύτερο αριθμό συνδεδεμένων αντικειμένων, η συσκευή ομίχλης μπορεί να χρησιμοποιεί κοντέινερ αντί για VM για να κατανέμει τις απαιτήσεις πόρων για κάθε συνδεδεμένο αντικείμενο. Η κύρια διαφορά μεταξύ μιας εικονικοποίησης που βασίζεται σε κοντέινερ και πλήρους εικονικοποίησης είναι το γεγονός ότι τα κοντέινερ μοιράζονται όχι μόνο το ίδιο υλικό αλλά και το ίδιο λειτουργικό σύστημα με τα άλλα εμπορευματοκιβώτια που φιλοξενούνται στην ίδια συσκευή ομίχλης. Να μοιράζεται το ίδιο λειτουργικό σύστημα μεταξύ των κοντέινερ που προορίζονται για αντικείμενα που ανήκουν σε διαφορετικούς χρήστες εγείρει σοβαρές ανησυχίες για την ασφάλεια, καθώς οι ευκαιρίες για διαρροή δεδομένων αυξάνονται σημαντικά.
- **Θέματα απορρήτου:** Αναφέραμε προηγουμένως ότι κάθε έξυπνο αντικείμενο θα είναι συνδεδεμένο με μία από τις συσκευές ομίχλης που βρίσκονται κοντά του. Αυτό σημαίνει ότι η συσκευή ομίχλης μπορεί να συμπεράνει τη θέση όλων των συνδεδεμένων έξυπνων αντικειμένων. Αυτό επιτρέπει στη συσκευή ομίχλης να παρακολουθεί χρήστες τους, γεγονός που μπορεί να παραβιάσει την ιδιωτικότητα των χρηστών που φέρουν αυτά τα αντικείμενα. Θα πρέπει να αναπτυχθούν νέοι μηχανισμοί προκειμένου να δυσχεραίνεται η παρακολούθηση της θέσης των έξυπνων αντικειμένων από τις συσκευές ομίχλης με την πάροδο του χρόνου. μια συσκευή που ονομάζεται obfuscator αποτρέπει τη διαρροή τέτοιων πληροφοριών εκπέμποντας σήματα που δυσκολεύουν έναν μη εξουσιοδοτημένο δέκτη να συμπεράνει το πλάτος, τη συχνότητα και τη χρονική μετατόπιση των αρχικά ανταλλαγμένων σημάτων.

## 4.3 Επιθέσεις και αντίμετρα στον τομέα της ανίχνευσης

Ο τομέας ανίχνευσης περιέχει όλα τα έξυπνα αντικείμενα, όπου κάθε αντικείμενο είναι εξοπλισμένο με έναν αριθμό αισθητήρων που επιτρέπουν στο αντικείμενο να αντιλαμβάνεται τον κόσμο. Τα έξυπνα αντικείμενα είναι επίσης εφοδιασμένα με μια διεπαφή επικοινωνίας που του επιτρέπει να επικοινωνεί με τον εξωτερικό κόσμο. Το έξυπνο αντικείμενο αναφέρει τα δεδομένα που αντιλαμβάνεται σε ένα από τα πεδία ομίχλης στον τομέα της ομίχλης. Αυτό γίνεται είτε με τη δημιουργία άμεσης σύνδεσης με τη συσκευή ομίχλης, είτε με τρόπο πολλαπλών βημάτων όπου το έξυπνο αντικείμενο βασίζεται σε άλλα έξυπνα αντικείμενα που βρίσκονται κατά μήκος της διαδρομής προς τη συσκευή ομίχλης για να παραδώσει τα δεδομένα που ανιχνεύονται[12]

Ο τομέας της ανίχνευσης είναι ευάλωτος σε πολλαπλές επιθέσεις. Ορισμένες από τις πιο γνωστές είναι:

### *4.3.1 Επίθεση παρεμβολής*

Αυτή η επίθεση προκαλεί διακοπή της υπηρεσίας και γίνεται με δύο τρόπους[12]:

- **Παρεμπόδιση του δέκτη:** Αυτή η επίθεση στοχεύει τον δέκτη, ένας κακόβουλος χρήστης εκπέμπει ένα σήμα το οποίο παρεμβαίνει στα νόμιμα σήματα που λαμβάνονται στον πλευρά του δέκτη. Η παρεμβολή υποβαθμίζει την ποιότητα του λαμβανόμενου σήματος προκαλώντας πολλά σφάλματα. Ως αποτέλεσμα, το άκρο λήψης δεν αναγνωρίζει τη λήψη αυτών των κατεστραμμένων πακέτων και περιμένει από τον αποστολέα να αναμεταδώσει αυτά τα πακέτα.
- **Παρεμπόδιση του αποστολέα:** Σε αντίθεση με την προηγούμενη επίθεση, αυτός ο τύπος στοχεύει τα αντικείμενα. Ο παρεμβολέας σε αυτή την επίθεση στέλνει ένα σήμα παρεμβολής που εμποδίζει τα γειτονικά αντικείμενα να μεταδώσουν τα πακέτα τους, καθώς αντιλαμβάνονται ότι το κανάλι είναι κατειλημμένο και αποσύρονται περιμένοντας το κανάλι να γίνει αδρανές.

Υπάρχουν διάφορες στρατηγικές παρεμβολής που μπορεί να ακολουθήσει ένας παρεμβολέας για να εξαπολύσει μια επίθεση. Οι πιο γνωστές από αυτές είναι[12]:

- **Συνεχής εμπλοκή:** Ο επιτιθέμενος εκπέμπει συνεχώς ένα τυχαίο σήμα παρεμβολής όλη την ώρα. Ο κύριος περιορισμός αυτής της επίθεσης είναι ότι μπορεί να ανιχνευθεί εύκολα παρατηρώντας τυχαία bits που δεν ακολουθούν το μοτίβο. Ένας άλλος κύριος περιορισμός είναι το γεγονός ότι η συσκευή παρεμβολής πρέπει να είναι συνδεδεμένη με μια πηγή ενέργειας, καθώς απαιτεί πολλή ενέργεια.
- **Παραπλανητική παρεμβολή:** Αυτό είναι παρόμοιο με τη συνεχή παρεμβολή, με την εξαίρεση ότι ότι ο παρεμβολέας αποκρύπτει την κακόβουλη συμπεριφορά του μεταδίδοντας νόμιμα πακέτα που ακολουθούν το μοτίβο αντί να στέλνει τυχαία bits.
- **Αντιδραστικές παρεμβολές:** Αυτή είναι μια στρατηγική για την παρεμβολή του δέκτη που είναι κατάλληλη για την περίπτωση που η συσκευή παρεμβολής έχει περιορισμένη ισχύς . Ο παρεμβολέας σε αυτή την περίπτωση ακούει το κανάλι και εκπέμπει ένα σήμα παρεμβολής μόνο αφού αισθάνεται ότι ένα νόμιμο σήμα μεταδίδεται. Αυτό είναι αποδοτικότερο από τη συνεχή μετάδοση σημάτων, καθώς η ακρόαση του καναλιού καταναλώνει λιγότερη ενέργεια από τη μετάδοση σημάτων.
- **Τυχαία παρεμβολή:** Ο παρεμβολέας εναλλάσσεται μεταξύ της αποστολής ενός σήματος παρεμβολής και παραμένοντας σε αδράνεια για τυχαίες χρονικές περιόδους, προκειμένου να αποκρύψει την κακόβουλη δραστηριότητα.

Υπάρχουν διάφορες προληπτικές και ανιχνευτικές τεχνικές για την αντιμετώπιση των παρεμβολών ε. Στη συνέχεια συνοψίζουμε τις πιο δημοφιλείς[12]:

- **Μεταπήδηση συχνότητας:** Αυτή είναι μια προληπτική τεχνική όπου ο πομπός και ο δέκτης αλλάζουν από μια συχνότητα σε μια άλλη προκειμένου να ξεφύγουν από κάθε πιθανή παρεμβολή.
- **Φάσμα διασποράς:** Αυτή η τεχνική χρησιμοποιεί μια ακολουθία μεταπήδησης που μετατρέπει το στενό σήμα σε σήμα με πολύ ευρεία ζώνη, γεγονός που καθιστά δυσκολότερο το γεγονός οι κακόβουλοι χρήστες να ανιχνεύσουν ή να μπλοκάρουν το σήμα.

- **Κατευθυντικές κεραίες:** Η χρήση κατευθυντικών κεραιών μπορεί να μετριάσει τις παρεμβολές καθώς οι κεραίες του αποστολέα και του δέκτη θα έχουν λιγότερη ευαισθησία στο θόρυβο που προέρχεται από τις τυχαίες κατευθύνσεις.
- **Ανίχνευση παρεμβολών:** Διαφορετικές τεχνικές ανίχνευσης έχουν προταθεί για την ανίχνευση επιθέσεων παρεμβολής. Ο δέκτης μπορεί να ανιχνεύσει ότι είναι θύμα μιας τέτοιας επίθεσης συλλέγοντας χαρακτηριστικά όπως η λαμβανόμενη ισχύς σήματος.

### *4.3.2 Επίθεση επιλεκτικής προώθησης*

Η επίθεση αυτή λαμβάνει χώρα στην περίπτωση που το αντικείμενο δεν μπορεί να στείλει τα παραγόμενα πακέτα του απευθείας στη συσκευή ομίχλης αλλά πρέπει να βασιστεί σε άλλα αντικείμενα που βρίσκονται κατά μήκος της διαδρομής προς τη συσκευή ομίχλης για να παραδώσουν αυτά τα πακέτα. Το κακόβουλο αντικείμενο σε αυτή την επίθεση δεν προωθεί ένα μέρος των πακέτων που λαμβάνει από τα γειτονικά αντικείμενα. Μια ειδική περίπτωση αυτής της επίθεσης είναι η Μαύρη Τρύπα όπου ο επιτιθέμενος απορρίπτει ολόκληρο το σύνολο των πακέτων που λαμβάνει από τα γειτονικά αντικείμενα. Ο καλύτερος τρόπος για να την αποτρέψετε είναι η αύξηση της ικανότητας μετάδοσης των αντικειμένων, ώστε να μπορούν να φτάνουν απευθείας στη συσκευή ομίχλης χωρίς να απαιτείται βοήθεια από ενδιάμεσα αντικείμενα. Ο Πλεονασμός Διαδρομής είναι μια ακόμη λύση, όπου κάθε αντικείμενο προωθεί κάθε παραγόμενο πακέτο σε πολλαπλά γειτονικά αντικείμενα, όπου πολλαπλά αντίγραφα του ίδιου πακέτου παραδίδονται στη συσκευή ομίχλης μέσω διαφορετικών διαδρομών. Αυτό το μειώνει τις πιθανότητες να μην υπάρχει τουλάχιστον ένα αντίγραφο κάθε παραγόμενου πακέτου να παραδοθεί στη συσκευή ομίχλης. Ο κύριος περιορισμός αυτής της τεχνικής μετριασμού είναι ότι έχει υψηλή ενεργειακή επιβάρυνση, καθώς αυξάνει σημαντικά την κυκλοφορία.[12]

### *4.3.3 Επίθεση σε καταβόθρα*

Ενα κακόβουλο αντικείμενο ισχυρίζεται ότι έχει τη συντομότερη διαδρομή προς την συσκευή ομίχλης και προσελκύει όλα τα γειτονικά αντικείμενα που δεν έχουν τη δυνατότητα μετάδοσης να φτάσουν στη συσκευή ομίχλης, να προωθήσουν τα πακέτα τους σε αυτό το κακόβουλο αντικείμενο και να βασίζονται σε αυτό το αντικείμενο για να παραδώσουν τα πακέτα τους. Τώρα όλα τα πακέτα που προέρχονται από τους γειτονικούς κόμβους περνούν από αυτόν τον κακόβουλο κόμβο. Αυτό το δίνει στον κακόβουλο κόμβο τη δυνατότητα να εξετάζει το περιεχόμενο όλων των προωθούμενων πακέτων, εάν τα δεδομένα αποστέλλονται χωρίς κρυπτογράφηση. Επιπλέον, το κακόβουλο αντικείμενο μπορεί να απορρίψει ορισμένα ή όλα τα λαμβανόμενα πακέτα, όπως εξηγήσαμε προηγουμένως. Τεχνικές ανίχνευσης και απομόνωσης των κακόβουλων αντικειμένων προτάθηκαν και βασίζονται στην ιδέα της συλλογής πληροφοριών από διάφορα αντικείμενα, όπου κάθε αντικείμενο αναφέρει τα γειτονικά αντικείμενα μαζί με την απόσταση μεταξύ τους. Ένα σύστημα ανίχνευση εισβολής χρησιμοποιείται στη συνέχεια για να βασιστεί σε αυτές τις πληροφορίες για τον εντοπισμό των αντικειμένων που ενδεχομένως να παρέχουν παραπλανητικές πληροφορίες. Η ανίχνευση μιας τέτοιας επίθεσης γίνεται δυσκολότερη όταν πολλαπλοί κακόβουλοι κόμβοι συνεργάζονται για να αποκρύψουν ο ένας τον άλλον.[12]

| Attack | Target OSI layer | Vulnerability reason | Security violation | Countermeasures |
|---|---|---|---|---|
| Jamming attack | Physical Data link | Shared wireless channel | Availability | Frequency hopping<br>Spread spectrum<br>Directional antennas<br>Jamming detection techniques |
| Selective-forwarding attack | Network | Limited transmission capability | Availability | Increase transmission range<br>Path redundancy<br>Choose certain intermediate objects as checkpoints to acknowledge received packets |
| Sinkhole attack | Network | Limited transmission capability | Confidentiality<br>Availability | Analyze the collected routing information from multiple objects |

Εικόνα 4.2 Επιθέσεις και αντίμετρα στον τομέα της ανίχνευσης[12]

# 5 Επίλογος

## 5.1 Σύνοψη και συμπεράσματα

Στην εργασία αυτή αναλύθηκε η ασφάλεια και η ιδιωτικότητα του IoT. Αγνοώντας αυτούς τους δύο παράγοντες θα περιοριστεί την εφαρμοσιμότητα του IoT και θα υπάρξουν σοβαρά αποτελέσματα στις διάφορες πτυχές της ζωής μας, δεδομένου ότι όλα τα φυσικά αντικείμενα στο περιβάλλον μας. Σε αυτό το κεφάλαιο, οι προκλήσεις για την ασφάλεια του IoT και οι προσδιορίστηκαν οι απαιτήσεις ασφάλειας του IoT. Επίσης αναλύθηκαν οι προκλήσεις για την ασφάλεια και οι απαιτήσεις ασφάλειας του IoT. Ακόμη εξετάστηκε η αρχιτεκτονική τριών τομέων, όπου αναλύσαμε τις επιθέσεις που στοχεύουν τους τρεις τομείς. Η ανάλυσή περιγράφει τις διαφορετικές επιθέσεις σε κάθε τομέα και ποια αμυντικά αντίμετρα μπορούν να εφαρμοστούν για την πρόληψη, την ανίχνευση ή τον μετριασμό αυτών των επιθέσεων. Τέλος, πρέπει η ασφάλεια και η προστασία της ιδιωτικότητα να λαμβάνονται υπόψη στο πρώιμο στάδιο σχεδιασμού του IoT, προκειμένου να αποφευχθεί η παγίδα να εξετάζεται η ασφάλεια ως μεταγενέστερη σκέψη.

## 5.2 Μελλοντικές Επεκτάσεις

Ακολουθούν ορισμένες από τις μελλοντικές κατευθύνσεις για την ασφάλεια του IoT και προστασία της ιδιωτικότητας.[13][14]

- **Ελαφριά κρυπτογραφία:** ο στόχος είναι να βρεθούν αποδοτικές τεχνικές κρυπτογράφησης που να μπορούν να αντικαταστήσουν τις παραδοσιακές υπολογιστικά δαπανηρές, επιτυγχάνοντας παράλληλα ένα αποδεκτό επίπεδο ασφάλειας.
- **Ασφάλεια τομέα ομίχλης:** Ο τομέας ομίχλης είναι ένας νέος τομέας που εισήχθη για να φέρει τις υπολογιστικές δυνατότητες στην άκρη του δικτύου. Πρέπει να δοθεί προσοχή σε αυτόν τον τομέα. Η εστίαση θα πρέπει να γίνει στον εντοπισμό μοντέλων απειλής που σχετίζονται με τον τομέα της ομίχλης και στην εξεύρεση αποτελεσματικών λύσεων.
- **Συνεργατική άμυνα:** μια συνεργατική λύση όπου οι διάφοροι τομείς (νέφος, ομίχλη και ανίχνευση) αλληλεπιδρούν μεταξύ τους για να σταματήσουν ή να μετριάσουν μια συγκεκριμένη επίθεση.

# Βιβλιογραφία


[1] Διαδίκτυο των πραγμάτων
(https://el.wikipedia.org/wiki/%CE%94%CE%B9%CE%B1%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%BF_%CF%84%CF%89%CE%BD_%CF%80%CF%81%CE%B1%CE%B3%CE%BC%CE%AC%CF%84%CF%89%CE%BD)

[2] Internet of things
(https://en.wikipedia.org/wiki/Internet_of_things)

[3] What is the IoT? Everything you need to know about the Internet of Things right now
(https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/)

[4] What is internet of things (IoT)?
https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[5] IoTPTS '15: Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security

[6] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 7-8

[7] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 212-214

[8] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 214

[9] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 215-216

[10] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 216-224

[11] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 224-227

[12] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 227-234

[13] Dabbagh M., Rayes A. (2019) Internet of Things Security and Privacy. In: Internet of Things From Hype to Reality. Springer, Cham. pp 235

[14] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, 2014, pp. 1-8, doi: 10.1109/PRISMS.2014.6970594.

[15] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[16] 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, 2019.

[17] C. Stergiou, K. E. Psannis, B.-G. Kim, B. Gupta, “Secure integration of IoT and Cloud Computing”, Elsevier, Future Generation Computer Systems, vol. 78, part 3, pp. 964-975, January 2018. [DOI:10.1016/j.future.2016.11.031]

[18] 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. [DOI: 10.1016/j.suscom.2018.06.003]

[19] Psannis, Kostas & Plageras, Andreas & Stergiou, Christos. (2019). "Internet of Things for Healthcare: Challenges & Perspectives". Invited lecture at International Summer School: Medical Law and Bioethics "HEALTH LAW AND THE INTERNET"