ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια σε IoT περιβάλλοντα και εφαρμογές

ΕΥΣΤΡΑΤΙΟΣ ΚΑΡΒΟΥΝΗΣ
Α.Μ. 711141262

Εισηγητής: << ΑΝΤΩΝΙΟΣ, ΜΠΟΓΡΗΣ, ΚΑΘΗΓΗΤΗΣ>>

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια σε IoT περιβάλλοντα και εφαρμογές

Ευστράτιος Καρβούνης
Α.Μ. 711141262

Εισηγητής:

<< ΑΝΤΩΝΙΟΣ, ΜΠΟΓΡΗΣ, ΚΑΘΗΓΗΤΗΣ>> Antonios Bogris Digitally signed by Antonios Bogris Date: 2023.10.11 22:01:35 +03'00'

Εξεταστική Επιτροπή:

Ioanna Kantzavelou Digitally signed by Ioanna Kantzavelou Date: 2023.10.12 08:42:09 +03'00'

<< ΙΩΑΝΝΑ, ΚΑΝΤΖΑΒΕΛΟΥ, ΕΠΙΚΟΥΡΗ ΚΑΘΗΓΗΤΡΙΑ>>
<< ΒΑΣΙΛΕΙΟΣ, ΜΑΜΑΛΗΣ, ΚΑΘΗΓΗΤΗΣ>>

Vasileios Mamalis Digitally signed by Vasileios Mamalis Date: 2023.10.16 08:20:50 +03'00'

Ημερομηνία εξέτασης
09/10/2023

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο/η κάτωθι υπογεγραμμένος Καρβούνης Ευστράτιος του Δημητρίου, με αριθμό μητρώου 711141262 φοιτητής του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Βεβαιώνω ότι είμαι συγγραφέας αυτής της Διπλωματικής εργασίας και κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

«Βεβαιώνω ότι είμαι συγγραφέας της παρούσας διπλωματικής εργασίας και ότι έχω αναφέρει ή παραπέμψει σε αυτή, ρητά και συγκεκριμένα, όλες τις πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, προτάσεων ή λέξεων, είτε αυτές μεταφέρονται επακριβώς (στο πρωτότυπο ή μεταφρασμένες) είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για την συγκεκριμένη διπλωματική εργασία»

Ο/Η Δηλών/ούσα

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω το εκπαιδευτικό προσωπικό του τμήματος Μηχανικών Πληροφορικής και Υπολογιστών. Επίσης θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέπων καθηγητή μου κ. Αντώνη Μπόγρη όπου είναι ένας εξαιρετικός εκπαιδευτικός και στήριξε την προσπάθειά μου, καθώς και την επίκουρη καθηγήτρια κ. Ιωάννα Καντζάβελου που μου έδωσε την πολύτιμη εμπειρία να συμμετέχω στην ερευνητική της ομάδα INSSec και να ανακαλύψω το ενδιαφέρον μου για την κυβερνοασφάλεια. Ακόμα θα ήθελα να ευχαριστήσω την οικογένειά μου για την υποστήριξη της που βοήθησε να ολοκληρώσω τις σπουδές μου.

ΠΕΡΙΛΗΨΗ

Στόχος της παρούσας διπλωματικής εργασίας είναι η Ασφάλεια στο Διαδίκτυο των Πραγμάτων έτσι ώστε ένας χρήστης να γνωρίζει πώς να προστατευτεί ή προστατέψει την περιουσία του από ηλεκτρονική κατασκοπεία ή απειλή από επιτιθέμενους στο δίκτυο του. Ακόμη θα γίνει βιβλιογραφική έρευνα σε πρωτόκολλα και συστήματα, όπως η τεχνική PUF, με σκοπό την αντιμετώπιση των θεμάτων ασφαλείας IoT.

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ Ασφάλεια

Κυβερνοασφάλεια,IoT security, Hardware security - physical unclonable functions (PUFs)

ABSTRACT

Thesis aims to give insight to the Internet of Things' user so that he knows how to protect himself or his property from electronic espionage or threat from attackers in his network. There will also be literature research on protocols and systems, such as the PUF technique, in order to counterfeit IoT security issues .

KEYWORDS

Cybersecurity, IoT security, Hardware security - physical unclonable functions (PUFs)

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

IoT	Internet of Things
DDoS	Dynamic Denial of Service
NIST	National Institute of Standards and Technology
PUF	Physical Unclonable Function
IDS	Intrusion Detection System
IDP	Intrusion Detection and Prevention
AES	Advanced Encryption Standard
RSA	Rivest-Shamir-Adleman
DES	Data Encryption Standard
DTLS	Datagram Transport Layer Security
SSH	Secure Shell
IPSec	IP Security
OTA	Over-the-Air
HSM	Hardware Security Module

1ο ΚΕΦΑΛΑΙΟ ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο αναλύεται το αντικείμενο της διπλωματικής εργασίας και γίνεται μια ιστορική αναδρομή γύρω από τις μεθόδους που έχουν παρουσιαστεί σε αυτήν την περιοχή.

1.1. Περιγραφή του αντικειμένου της διπλωματικής εργασίας

Η Ασφάλεια στο Διαδίκτυο των Πραγμάτων (Internet of Things - IoT) αναφέρεται στο σύνολο των μέτρων και τεχνικών που χρησιμοποιούνται για την προστασία των συσκευών και των δεδομένων που συνδέονται στο διαδίκτυο μέσω του IoT. Αυτό περιλαμβάνει την προστασία από δυνητικές απειλές, όπως κακόβουλο λογισμικό, επιθέσεις χάκερ, παραβίαση απορρήτου και ανεπιθύμητη παρείσφρηση στα συστήματα.

Καθώς οι έξυπνες συσκευές γίνονται όλο και πιο διαδεδομένες και συνδέονται μεταξύ τους και με το διαδίκτυο, η ασφάλεια στο IoT γίνεται ολοένα και σημαντικότερη. Οι επιθέσεις στο IoT μπορούν να έχουν αρνητικές συνέπειες, όπως τη διαρροή προσωπικών δεδομένων, την απειλή για την ασφάλεια του χρήστη ή την παραβίαση της λειτουργίας των συσκευών.

Για την επίτευξη ασφάλειας στο IoT, μπορούν να εφαρμοστούν διάφορα μέτρα, όπως η χρήση ισχυρών κωδικών πρόσβασης, η αναβάθμιση και ενημέρωση του λογισμικού των συσκευών για την επιδιόρθωση προβλημάτων ασφαλείας, η κρυπτογράφηση των δεδομένων, η επιλογή αξιόπιστων προμηθευτών συσκευών και η δικτυακή ασφάλεια με τη χρήση τεχνολογιών, όπως πρότυπα ελέγχου πρόσβασης και προηγμένων μηχανισμών ανίχνευσης και αντιμετώπισης απειλών.

Γενικά, η ασφάλεια στο IoT απαιτεί συνεχή προσοχή και προληπτικά μέτρα από τους χρήστες, τους κατασκευαστές συσκευών και τους παρόχους υπηρεσιών για να διασφαλίσουν την προστασία των δεδομένων και την ασφάλεια του συνδεδεμένου περιβάλλοντος.

1.2. Ιστορική αναδρομή

Η ασφάλεια στο Διαδίκτυο των Πραγμάτων (IoT) έχει εξελιχθεί σταδιακά μαζί με την εξάπλωση και την υιοθέτηση της τεχνολογίας IoT. Ας ρίξουμε μια ματιά σε μερικά κλασικά παραδείγματα και γεγονότα που συνέβησαν στην ιστορία της ασφάλειας του IoT:

- Αρχικά, η ασφάλεια δεν ήταν προτεραιότητα: Κατά την εκκίνηση της τεχνολογίας IoT, η ασφάλεια δεν ήταν πάντα η κύρια ανησυχία. Πολλές έξυπνες συσκευές και αισθητήρες δημιουργήθηκαν με αδυναμίες ασφαλείας και αυτό δημιούργησε ευπάθειες στο σύστημα.

- Επιθέσεις Mirai Botnet: Το 2016, η επίθεση Mirai Botnet έλαβε χώρα, όπου κακόβουλο λογισμικό εκμεταλλεύτηκε αδύναμες ασφαλείς προεπιλογές και κωδικούς πρόσβασης σε έξυπνες συσκευές IoT για να δημιουργήσει ένα μεγάλο botnet. Αυτό το botnet χρησιμοποιήθηκε σε μαζικές επιθέσεις DDoS, προκαλώντας προβλήματα σε διάφορες ιστοσελίδες.
- Οδηγίες για την ασφάλεια του IoT: Διάφοροι οργανισμοί και εταιρείες ασφαλείας έχουν αναπτύξει οδηγίες και πρακτικές για τη βελτίωση της ασφάλειας του IoT. Παραδείγματα περιλαμβάνουν το Internet of Things Project και τις οδηγίες ασφαλείας του NIST (National Institute of Standards and Technology) για το IoT.
- Ευαισθητοποίηση για την ασφάλεια: Οι σοβαρές παραβιάσεις ασφαλείας και οι επιθέσεις στο IoT έχουν αυξήσει την ευαισθητοποίηση και την ανάγκη για καλύτερη ασφάλεια. Οι κατασκευαστές συσκευών IoT και οι πάροχοι υπηρεσιών έχουν αρχίσει να δίνουν μεγαλύτερη έμφαση στην ασφάλεια και να ενσωματώνουν περισσότερα μέτρα προστασίας.
- Νομοθεσία για την ασφάλεια του IoT: Ορισμένες χώρες έχουν ξεκινήσει να επιβάλλουν νομοθεσία για την ασφάλεια του IoT. Για παράδειγμα, η Καλιφόρνια στις Ηνωμένες Πολιτείες έχει θεσπίσει τον νόμο SB-327, που απαιτεί από τους κατασκευαστές να εφαρμόζουν ασφάλεια στις συσκευές IoT που διατίθενται στην αγορά της πολιτείας.

Αξίζει να σημειωθεί ότι η ασφάλεια του IoT εξακολουθεί να είναι ένας δυναμικά εξελισσόμενος τομέας, και η έρευνα και οι προσπάθειες για βελτίωση της ασφάλειας συνεχίζονται.

1.3. Στόχος και σκοπός της Εργασίας

Το ερευνητικό ερώτημα που διατρέχει την εργασία είναι να εντοπισθούν οι πρακτικές ασφαλείας που συμβάλουν στην αύξηση της ασφάλειας σε περιβάλλον IoT. Ειδικότερα θα διερευνηθεί αν μία πρακτική μπορεί να λύσει συνολικά το πρόβλημα της ασφάλειας των IoT συσκευών και ειδικότερα αν τεχνικές ενσωματωμένες σε υλικό (embedded), όπως των φυσικά μη κλωνοποιήσιμων συναρτήσεων (PUFs), συμβάλουν σε αυτή την κατεύθυνση.

1.3.1 Physical Unclonable Functions (PUFs)

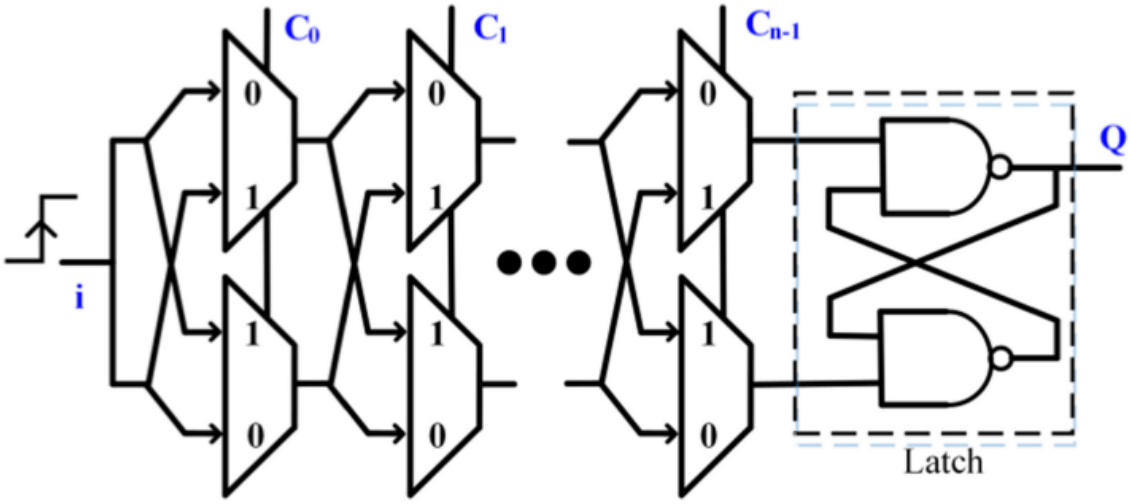
Οι φυσικά μη κλωνοποιήσιμες συναρτήσεις (Physical Unclonable Functions - PUFs) είναι μηχανισμοί που χρησιμοποιούνται για να ενισχύσουν την ασφάλεια του Internet of Things (IoT). Τα PUFs είναι μηχανισμοί βασισμένοι σε υλικό (embedded) που εκμεταλλεύονται τυχαίες παραλλαγές στα φυσικά χαρακτηριστικά των συσκευών για τη δημιουργία μοναδικών αναγνωριστικών κλειδιών.

Τα PUFs λειτουργούν ως προσωρινά μη αναπαραστατικά κλειδιά, καθώς εξάγουν μοναδικά ψηφία από το περιβάλλον εκκίνησης και τη φυσική δομή του υλικού. Αυτά τα ψηφία μπορούν να χρησιμοποιηθούν ως βάση για τη δημιουργία κλειδιών κρυπτογράφησης, την πιστοποίηση των συσκευών ή την επαλήθευση της γνησιότητας τους. Η χρήση των PUFs επηρεάζει την ασφάλεια του IoT με τους εξής τρόπους:

- Τα PUFs δημιουργούν μοναδικά αναγνωριστικά κλειδιά για κάθε συσκευή IoT. Αυτό εξασφαλίζει ότι κάθε συσκευή έχει μοναδικό αναγνωριστικό κλειδί, προστατεύοντας έτσι από επιθέσεις όπως οι επιθέσεις αντιγραφής ή απομάκρυνσης.
- Τα PUFs είναι ανθεκτικά στις επιθέσεις καθώς βασίζονται σε μη αναπαράστατα χαρακτηριστικά των συσκευών. Αυτό καθιστά δυσκολότερη την αποτύπωση και αντιγραφή των κλειδιών.
- Τα PUFs έχουν ελάχιστες απαιτήσεις χωρητικότητας αποθήκευσης για κλειδιά, καθώς τα κλειδιά παράγονται κατά τη διάρκεια της λειτουργίας του συστήματος. Αυτό μειώνει τον κίνδυνο αποκάλυψης των κλειδιών από φυσική κλοπή ή κακόβουλο λογισμικό.

Ωστόσο, πρέπει να σημειωθεί ότι τα PUFs δεν είναι απόλυτα άρρηκτα ασφαλείς. Μπορούν να επηρεαστούν από φυσικές μεταβολές, θερμοκρασία, φθορά και άλλους παράγοντες που μπορεί να οδηγήσουν σε σφάλματα ή ανακάλυψη των κλειδιών. Επίσης, οι επιθέσεις που στοχεύουν τον περιβάλλοντα χώρο του PUF (όπως η εισαγωγή θορύβου) μπορούν να επηρεάσουν την ασφάλεια του.

Στο ακόλουθο Σχήμα 1 αναπαρίσταται σε απλοϊκή μορφή ένας μηχανισμός παραγωγής ακολουθίας Bit κατά PUF με βάση το υλικό. Τα bit ελέγχου (C) οδηγούν τους μεμονωμένους πολυπλέκτες και προκαλούν διαφορετικές καθυστερήσεις στο σήμα εισόδου με κατά συνέπεια η τιμή της εξόδου του μηχανισμού PUF (Q) να διαφέρει.



Σχήμα 1 Διάταξη παραγωγής ακολουθίας bit από PUF [14].

1.4. Δομή και περιεχόμενο της Διπλωματικής

Η διπλωματική αναλύεται σε 5 κεφάλαια. Στο πρώτο κεφάλαιο παραθέτουμε το στόχο και σκοπό της Διπλωματικής και αναλύουμε την ιστορική διαδρομή μέχρι σήμερα. Στο δεύτερο κεφάλαιο αναλύουμε τα προβλήματα ασφαλείας ώστε να σχηματιστεί το γνωστικό υπόβαθρο πάνω στο οποίο θα αναπτυχθεί το αντικείμενο της Διπλωματικής. Στο τρίτο κεφάλαιο διερευνούμε τα προβλήματα ασφαλείας που παρουσιάζονται σε περιβάλλοντα που εμπεριέχουν συσκευές IoT καθώς και στις ίδιες τις συσκευές.

Στο τέταρτο κεφάλαιο παρουσιάζουμε βάση της βιβλιογραφίας τις σημαντικότερες πρακτικές αντιμετώπισης των θεμάτων ασφαλείας και συγκρίνουμε τα χαρακτηριστικά τους. Στο πέμπτο κεφάλαιο παραθέτουμε τα συμπεράσματα και τις εμπειρίες από την εκπόνησης της Διπλωματικής.

2ο ΚΕΦΑΛΑΙΟ ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΤΕΧΝΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Στο παρόν κεφάλαιο παρουσιάζονται οι τεχνικές ασφαλείας σε περιβάλλον IoT. Οι τεχνικές αυτές επιτρέπουν στις συσκευές IoT να παρέχουν ένα επίπεδο ασφάλειας και στα σχετιζόμενα με αυτές περιβάλλοντα ένα μηχανισμό διασφάλισης.

2.1. Εισαγωγή

Η ασφάλεια των υπολογιστικών συστημάτων αποτελεί έναν κρίσιμο παράγοντα για την προστασία των δεδομένων και την εξασφάλιση της ιδιωτικότητας και της ακεραιότητας των πληροφοριών. Με την έλευση του IoT και τη συνδεσιμότητα διάφορων συσκευών, η ανάγκη για ασφάλεια σε αυτά τα συστήματα έχει αυξηθεί ακόμα περισσότερο. Σε αυτό το κεφάλαιο, θα εξετάσουμε διάφορες τεχνικές ασφάλειας που μπορούν να εφαρμοστούν στα υπολογιστικά συστήματα για την προστασία τους από πιθανές απειλές:

1. **Ανίχνευση και πρόληψη εισβολών**: Η ανίχνευση και η πρόληψη εισβολών είναι μια τεχνική που αποσκοπεί στον εντοπισμό και την αποτροπή μη εξουσιοδοτημένων προσπαθειών πρόσβασης σε ένα υπολογιστικό σύστημα. Συνδυάζει τη χρήση συστημάτων ανίχνευσης εισβολών (IDS) και συστημάτων πρόληψης εισβολών (IPS) και μπορεί να βοηθήσει στον εντοπισμό και τον αποκλεισμό των κακόβουλων ενεργειών πριν προκαλέσουν ζημιά.
2. **Κρυπτογράφηση**: Η κρυπτογράφηση αποτελεί ένα από τα βασικά μέσα για την προστασία των δεδομένων. Με τη χρήση κρυπτογραφικών αλγορίθμων, τα δεδομένα μπορούν να κρυπτογραφηθούν και να μεταδοθούν με ασφάλεια, εξασφαλίζοντας ότι μόνο οι εξουσιοδοτημένοι αποδέκτες έχουν πρόσβαση σε αυτά. Επίσης, η κρυπτογράφηση μπορεί να χρησιμοποιηθεί για την αποθήκευση και τον προστατευτικό περιτύλιγμα των ευαίσθητων δεδομένων σε μια συσκευή IoT.
3. **Ενημέρωση και παρακολούθηση λογισμικού**: Η ενημέρωση και η παρακολούθηση του λογισμικού είναι ζωτικής σημασίας για την ασφάλεια των υπολογιστικών συστημάτων. Οι παραγωγοί λογισμικού πρέπει να παρέχουν τακτικά αναβαθμίσεις και ενημερώσεις για το λογισμικό τους, συμπεριλαμβανομένων των διορθώσεων ασφαλείας. Τα συστήματα IoT πρέπει να είναι σε θέση να ανιχνεύουν και να εγκαθιστούν αυτόματα αυτές τις ενημερώσεις για να διατηρούνται ενημερωμένα και προστατευμένα.
4. **Προσδιορισμός και επαλήθευση ταυτότητας**: Η προσδιορισμός και η επαλήθευση της ταυτότητας των συσκευών και των χρηστών αποτελούν σημαντικές τεχνικές ασφάλειας για τα υπολογιστικά συστήματα. Οι συσκευές IoT πρέπει να έχουν μοναδικές ταυτότητες και πιστοποιητικά για να αποτρέπεται η παραποίηση ή η απομίμησή τους. Επίσης, η επαλήθευση της ταυτότητας των χρηστών μέσω πιστοποιητικών, διαπιστευτηρίων και πολυπαραγοντικών μεθόδων μπορεί να εξασφαλίσει ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα συστήματα.

5. **Απομόνωση και εφαρμογή αρχών του ελάχιστου προνομίου**: Η απομόνωση των συστημάτων και η εφαρμογή αρχών του ελάχιστου προνομίου αποτελούν αποτελεσματικές τεχνικές για την προστασία των υπολογιστικών συστημάτων. Με την απομόνωση, διαφορετικά συστήματα και συσκευές μπορούν να λειτουργούν ανεξάρτητα ο ένας από τον άλλον, μειώνοντας τον κίνδυνο εξάπλωσης μιας επίθεσης. Επίσης, η εφαρμογή αρχών του ελάχιστου προνομίου περιορίζει τις δυνατότητες πρόσβασης και εκτέλεσης εντολών για τους χρήστες και τις συσκευές, μειώνοντας την επιθετική επιφάνεια.

2.2. Η ανίχνευση και η πρόληψη εισβολών (IDP)

Η ανίχνευση και η πρόληψη εισβολών (Intrusion Detection and Prevention, IDP) αποτελεί σημαντική τεχνική ασφαλείας υπολογιστικών συστημάτων που επιτρέπει τον εντοπισμό και τον περιορισμό των ανεπιθύμητων ενεργειών και εισβολών σε ένα σύστημα ή σε ένα δίκτυο. Η τεχνική βασίζεται σε διπλό μηχανισμό ασφαλείας, ο ένας αφορά την ανίχνευση των εισβολών και ο άλλος την πρόληψη τους.

2.2.1. Ανίχνευση εισβολών

Η ανίχνευση εισβολών (Intrusion Detection Systems - IDS) αφορά τον εντοπισμό ανεπιθύμητων, ή κακόβουλων ενεργειών που προκαλούνται από εξωτερικούς ή ακόμα και εσωτερικούς χρήστες. Οι τεχνικές ανίχνευσης εισβολών αναλύονται σε μια σειρά μεθόδων και τεχνικών, συμπεριλαμβανομένων ενδεικτικά και όχι αποκλειστικά των εξής:

- Η ανίχνευση ανωμαλιών ασχολείται με την αναγνώριση μη συνηθισμένων, ανεπιθύμητων προτύπων συμπεριφοράς στο σύστημα. Αυτές οι ανωμαλίες μπορεί να είναι αποτέλεσμα κακόβουλων ενεργειών, όπως δοκιμές χάκερ ή μη εξουσιοδοτημένη πρόσβαση, αλλά μπορεί επίσης να οφείλονται σε τεχνικά προβλήματα ή σφάλματα.
- Η ανίχνευση υπογραφών επικεντρώνεται στον εντοπισμό γνωστών προτύπων επιθέσεων ή κακόβουλου κώδικα που έχει ήδη αναγνωριστεί. Αυτές οι υπογραφές βασίζονται σε γνωστά χαρακτηριστικά επιθέσεων και αναγνωρίζονται από συστήματα IDS/IPS (Intrusion Detection/Prevention Systems).
- Η χρήση μηχανών μάθησης και αλγορίθμων νευρωνικών δικτύων μπορεί να βοηθήσει στην ανίχνευση μη πρωτότυπων εισβολών. Αυτές οι τεχνικές αναλύουν μεγάλες ποσότητες δεδομένων για να αναγνωρίσουν πρότυπα και να εντοπίσουν ανωμαλίες που μπορούν να υποδείξουν κακόβουλη δραστηριότητα.

Τα IDS που βασίζονται σε νευρωνικά δίκτυα επηρεάζουν την ασφάλεια του IoT με τους εξής τρόπους:

- Τα IDS που χρησιμοποιούν νευρωνικά δίκτυα μπορούν να ανιχνεύσουν ανωμαλίες στη συμπεριφορά των συσκευών IoT. Χρησιμοποιώντας μοντέλα μηχανικής μάθησης, τα νευρωνικά

δίκτυα μπορούν να εκπαιδευτούν να αναγνωρίζουν τα πρότυπα συμπεριφοράς των συσκευών και να εντοπίζουν ανεπιθύμητες, μη αναμενόμενες ή κακόβουλες ενέργειες. Αυτό μπορεί να βοηθήσει στην ανίχνευση επιθέσεων και στην πρόληψη μη εξουσιοδοτημένης πρόσβασης του συστήματος.

- Μπορούν επίσης να εκπαιδευτούν να αναγνωρίζουν γνωστά μοτίβα και σημάδια κακόβουλης δραστηριότητας. Αυτό σημαίνει ότι μπορούν να αναγνωρίσουν γνωστές απειλές και επιθέσεις που έχουν καταγραφεί και αναλυθεί προηγουμένως. Με τη χρήση νευρωνικών δικτύων, τα IDS μπορούν να εντοπίσουν τις ανωμαλίες στην εισερχόμενη κυκλοφορία δεδομένων και να αναλάβουν κατάλληλα μέτρα ασφαλείας.
- Τα νευρωνικά δίκτυα μεγάλου βάθους εκμάθησης (deep learning) μπορούν να εκπαιδευτούν και να αναγνωρίζουν πολύπλοκα μοτίβα και συμπεριφορές. Αυτό καθιστά δυνατή την ανίχνευση εξελισσόμενων και εξεζητημένων απειλών που μπορεί να μην έχουν προηγουμένως καταγραφεί ή αναγνωριστεί.

Συνολικά, η χρήση των IDS με νευρωνικά δίκτυα μπορεί να βελτιώσει την ασφάλεια του IoT προσφέροντας προηγμένες ικανότητες ανίχνευσης και αναγνώρισης κακόβουλων ενεργειών, είτε είναι γνωστές είτε αναδυόμενες απειλές.

2.2.2. Πρόληψη εισβολών

Η πρόληψη εισβολών συνδυάζει την ανίχνευση εισβολών με την όπου είναι δυνατόν αποτροπή ή και τον περιορισμό των ανεπιθύμητων ενεργειών. Αυτό μπορεί να επιτευχθεί μέσω των εξής τεχνικών:

1. Απόκριση σε εισβολές (Intrusion Response): Μετά τον εντοπισμό μιας εισβολής, ακολουθείται μια διαδικασία απόκρισης που περιλαμβάνει την ειδοποίηση του αρμόδιου προσωπικού ασφαλείας, την απομόνωση του επιτιθέμενου συστήματος ή χρήστη και την αποτροπή περαιτέρω ζημιών ή πρόσβασης. Η ανάπτυξη μηχανισμών απόκρισης σε εισβολές για το IoT απαιτεί τη συνδυασμένη χρήση τεχνολογιών ανίχνευσης εισβολών, ευφυών αλγορίθμων και αυτοματοποιημένων διαδικασιών για να αντιμετωπιστεί η απειλή με αποτελεσματικό τρόπο. Οι μηχανισμοί απόκρισης σε εισβολές μπορούν να περιλαμβάνουν τα εξής [1]:

    - Ανιχνεύοντας μια εισβολή σε μια συσκευή, η αυτοματοποιημένη απόκριση μπορεί αυτόματα να περιορίσει την επικοινωνία της συσκευής με το υπόλοιπο σύστημα ή να την απομονώσει εντελώς για να αποτραπεί η εξάπλωση της απειλής.
    - Μια πλατφόρμα IoT μπορεί να λάβει αποφάσεις αυτόνομα για την απενεργοποίηση μιας συσκευής ή την εκτέλεση ενός συγκεκριμένου μέτρου προστασίας όταν παραβιάζονται πολιτικές ασφαλείας.
    - Μηχανισμοί απόκρισης σε εισβολές μπορούν να ειδοποιούν τους διαχειριστές ή τους χρήστες για την εντοπισμένη απειλή και να παρέχουν σχετικές πληροφορίες για την αντίδραση (απόκριση) που απαιτείται.

2. Φραγή της εισόδου (Intrusion Prevention): Τα συστήματα ανίχνευσης και πρόληψης εισβολών μπορούν να εφαρμόσουν μηχανισμούς φραγής για να περιορίσουν την πρόσβαση των επιτιθέμενων χρηστών ή συσκευών. Αυτό μπορεί να γίνει με τον αποκλεισμό της IP διεύθυνσης, την απόρριψη της πρόσβασης σε συγκεκριμένους πόρους ή την εφαρμογή περιορισμών στις εντολές που μπορούν να εκτελέσουν οι χρήστες. Οι μηχανισμοί αποκλεισμού εισόδου μπορούν να περιλαμβάνουν τις εξής τεχνικές [2]:

    - Η χρήση φίλτρων firewall μπορεί να περιορίσει την είσοδο πακέτων στο σύστημα IoT με βάση κανόνες που ορίζονται από τον διαχειριστή. Αυτό μπορεί να περιλαμβάνει τον περιορισμό της πρόσβασης από συγκεκριμένες διευθύνσεις IP, τον έλεγχο των πορτών εισόδου ή την εφαρμογή πολιτικών ασφαλείας.
    - Συστήματα αποκλεισμού εισόδου κακόβουλου λογισμικού (Malware) μπορούν να ανιχνεύουν την παρουσία κακόβουλου λογισμικού στο σύστημα IoT και να προβαίνουν σε αυτόματο μπλοκάρισμα ή απομάκρυνσή του.
    - Οι μηχανισμοί αποκλεισμού εισόδου μπορούν να εφαρμόζουν περιορισμούς στα εισερχόμενα δεδομένα προκειμένου να αποτραπεί η εισροή κακόβουλου περιεχομένου ή δεδομένων που μπορεί να προκαλέσουν ευπάθειες.

Ο συνδυασμός των τεχνικών ανίχνευσης και πρόληψης εισβολών είναι σημαντικός για την ασφάλεια υπολογιστικών συστημάτων. Η ανίχνευση εισβολών προσφέρει τη δυνατότητα ανίχνευσης απειλών και ανωμαλιών, ενώ η πρόληψη εισβολών επιτρέπει την άμεση αντίδραση και περιορισμό των ανεπιθύμητων ενεργειών. Με την ολοκληρωμένη εφαρμογή αυτών των τεχνικών, επιτυγχάνεται μια πιο ολοκληρωμένη και αποτελεσματική προστασία των υπολογιστικών συστημάτων.

2.3. Κρυπτογράφηση

Η κρυπτογραφία αποτελεί την επιστήμη και την τεχνική της μετατροπής πληροφορίας σε μορφή μη κατανοητού κειμένου, γνωστού ως κρυπτογραφημένο κείμενο, ώστε να προστατεύεται από μη εξουσιοδοτημένη πρόσβαση ή ανεπιθύμητη αποκάλυψη. Η κρυπτογραφία εφαρμόζεται σε διάφορους τομείς, όπως οι επικοινωνίες, η ασφάλεια δεδομένων και οι ψηφιακές υπογραφές, προσφέροντας απόρρητο, αυθεντικότητα και ακεραιότητα.

Υπάρχουν δύο βασικές κατηγορίες κρυπτογραφίας:

1. Συμμετρική κρυπτογραφία: Στη συμμετρική κρυπτογραφία, η ίδια κλειδούχος πληροφορία χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων. Ο αποστολέας και ο παραλήπτης πρέπει να μοιράζονται το ίδιο κλειδί. Η συμμετρική κρυπτογραφία είναι γρήγορη και αποτελεσματική για την κρυπτογράφηση μεγάλων όγκων δεδομένων, αλλά απαιτεί ασφαλή διανομή του κλειδιού.

2. Ασύμμετρη Κρυπτογραφία: Στην ασύμμετρη κρυπτογραφία, χρησιμοποιούνται διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων. Το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση των δεδομένων και παραμένει μυστικό στον κάτοχό του, ενώ το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση των δεδομένων και μπορεί να γνωστοποιηθεί σε οποιονδήποτε. Η ασύμμετρη κρυπτογραφία είναι πιο ασφαλής και επιτρέπει τη δημιουργία ψηφιακών υπογραφών.

Η κρυπτογραφία εφαρμόζεται σε διάφορα πρωτόκολλα και αλγορίθμους, όπως το AES (Advanced Encryption Standard), το RSA (Rivest-Shamir-Adleman), το DES (Data Encryption Standard) και πολλά άλλα. Οι επιλογές κρυπτογραφικών αλγορίθμων εξαρτώνται από τις απαιτήσεις ασφάλειας, την απόδοση και το περιβάλλον εφαρμογής.

- Η κρυπτογραφία AES [3] στο πλαίσιο του IoT έχει ευρεία εφαρμογή και μπορεί να βελτιώσει σημαντικά την ασφάλεια των συσκευών και των δεδομένων τους. Ένα παράδειγμα εφαρμογής του AES στο IoT είναι η κρυπτογράφηση των αισθητήρων και των δεδομένων που συλλέγονται από αυτούς, προτού αυτά μεταδοθούν στον προορισμό τους.
- Η κρυπτογραφία RSA [4] είναι ένα ασύμμετρο κρυπτογραφικό σύστημα που βασίζεται στη χρήση δύο κλειδιών, ενός ιδιωτικού κλειδιού για την αποκρυπτογράφηση και ενός δημόσιου κλειδιού για την κρυπτογράφηση. Η εφαρμογή του RSA στο πλαίσιο του IoT μπορεί να παρέχει ασφάλεια στις επικοινωνίες και την αυθεντικοποίηση των συσκευών.
- Ο αλγόριθμος κρυπτογράφησης DES (Data Encryption Standard) [5] είναι ένας κλασικός συμμετρικός αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση δεδομένων. Παρά το γεγονός ότι ο DES έχει χρησιμοποιηθεί ευρέως στο παρελθόν, θεωρείται πλέον ανασφαλής για πολλές εφαρμογές λόγω του μικρού μήκους των κλειδιών του. Στο πλαίσιο του IoT, η εφαρμογή του DES δεν συνιστάται λόγω της περιορισμένης ασφάλειας του. Αντ' αυτού, συνήθως χρησιμοποιούνται πιο ασφαλείς αλγόριθμοι, όπως το AES που αναφέρθηκε προηγουμένως. Ο AES παρέχει μεγαλύτερο μήκος κλειδιού και ασφαλέστερη κρυπτογράφηση από το DES.

Η κρυπτογραφία στο πλαίσιο του IoT εφαρμόζεται σε πολλούς τομείς και επιφέρει ουσιαστικά οφέλη για την ασφάλεια και την προστασία των δεδομένων. Ορισμένες σημαντικές εφαρμογές της κρυπτογραφίας στα IoT περιλαμβάνουν:

- Επικοινωνία μεταξύ συσκευών: Η κρυπτογραφία χρησιμοποιείται για την ασφαλή και εμπιστευτική (απόρρητη) επικοινωνία μεταξύ των συσκευών IoT. Αυτό διασφαλίζει ότι οι πληροφορίες που ανταλλάσσονται μεταξύ των συσκευών παραμένουν ασφαλείς από επιθέσεις και ανεπιθύμητη παρακολούθηση.
- Αυθεντικοποίηση και πιστοποίηση: Η κρυπτογραφία χρησιμοποιείται για την αυθεντικοποίηση και πιστοποίηση των συσκευών IoT. Μέσω της δημιουργίας και ανταλλαγής κρυπτογραφημένων πιστοποιητικών, οι συσκευές μπορούν να επαληθεύουν την ταυτότητα

ορισμένων συσκευών και να διασφαλίζουν ότι οι επικοινωνίες γίνονται με αξιόπιστους παράγοντες.

- Προστασία των δεδομένων: Η κρυπτογραφία χρησιμοποιείται για την προστασία των δεδομένων που αποθηκεύονται στις συσκευές IoT (at rest) και κατά την μεταφορά τους στο δίκτυο (on transit). Αυτό εμποδίζει την ανεπιθύμητη πρόσβαση και τη διαρροή των ευαίσθητων πληροφοριών.
- Απομόνωση και ασφάλεια δικαιωμάτων πρόσβασης: Η κρυπτογραφία μπορεί να χρησιμοποιηθεί για την απομόνωση και την ασφάλεια των δικαιωμάτων πρόσβασης στις συσκευές IoT. Μέσω κρυπτογραφημένων πρωτοκόλλων και κλειδιών πρόσβασης, εξασφαλίζεται ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις συσκευές και τα δεδομένα τους.
- Υπογραφές και ακεραιότητα δεδομένων: Η κρυπτογραφία μπορεί να χρησιμοποιηθεί για τη δημιουργία ψηφιακών υπογραφών και την επαλήθευση της ακεραιότητας των δεδομένων. Με την χρήση κρυπτογραφικών αλγορίθμων και κλειδιών, μπορούν να δημιουργηθούν ψηφιακές υπογραφές που επαληθεύουν ότι τα δεδομένα δεν έχουν παραβιαστεί ή αλλοιωθεί κατά τη μετάβαση από την αρχική συσκευή.

Υπάρχουν πολλά πρωτόκολλα που χρησιμοποιούνται στην κρυπτογραφία στο πλαίσιο του IoT. Ας δούμε ορισμένα παραδείγματα:

- Το πρωτόκολλο Transport Layer Security (TLS) είναι ένα από τα κύρια πρωτόκολλα κρυπτογράφησης που χρησιμοποιούνται για την ασφαλή επικοινωνία μεταξύ συσκευών IoT και διακομιστή. Παρέχει αυθεντικοποίηση, ακεραιότητα δεδομένων και απόρρητη επικοινωνία μέσω της κρυπτογράφησης των δεδομένων που ανταλλάσσονται.
- Το πρωτόκολλο Datagram Transport Layer Security (DTLS) είναι μια παραλλαγή του TLS που προσαρμόζεται για το περιβάλλον του IoT, όπου η απώλεια πακέτων και οι καθυστερήσεις είναι συχνό φαινόμενο. Χρησιμοποιείται για την ασφαλή μετάδοση δεδομένων μεταξύ συσκευών IoT και διακομιστή, διασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.
- Το πρωτόκολλο IP Security (IPSec) παρέχει ασφάλεια στο επίπεδο του διαδικτύου, προστατεύοντας την επικοινωνία μεταξύ συσκευών IoT. Χρησιμοποιείται για τη δημιουργία εικονικών ιδιωτικών δικτύων (VPN) και την κρυπτογράφηση των δεδομένων που μεταδίδονται μεταξύ των συσκευών.
- Το πρωτόκολλο Secure Shell (SSH) παρέχει ασφαλή απομακρυσμένη πρόσβαση σε συσκευές IoT. Χρησιμοποιεί κρυπτογραφία για την αυθεντικοποίηση των χρηστών, την προστασία των επικοινωνιών και την αποτροπή ανεπιθύμητης πρόσβασης στις συσκευές.

2.4. Ενημέρωση και παρακολούθηση λογισμικού

Η ενημέρωση και παρακολούθηση του λογισμικού σε συστήματα IoT είναι κρίσιμη για τη διασφάλιση της ασφάλειας και της αξιοπιστίας των συσκευών. Αυτή η διαδικασία περιλαμβάνει την ενημέρωση του λογισμικού σε κάθε συσκευή IoT με τις τελευταίες εκδόσεις και διορθώσεις ασφαλείας, καθώς και την παρακολούθηση της κατάστασης και της απόδοσης του λογισμικού στον χρόνο. Οι παρακάτω τεχνικές και πρακτικές χρησιμοποιούνται στην ενημέρωση και παρακολούθηση του λογισμικού στα συστήματα IoT [6]:

1. Η τεχνική Over-the-Air (OTA) ενημερώσεων επιτρέπει την ασύρματη ενημέρωση του λογισμικού σε συσκευές IoT. Αυτό επιτρέπει την εύκολη και αποτελεσματική αναβάθμιση του λογισμικού χωρίς την ανάγκη για φυσική παρέμβαση στη συσκευή. Οι ενημερώσεις OTA πρέπει να είναι ασφαλείς και αξιόπιστες για να αποτρέψουν τη δυνατότητα κακόβουλων επιθέσεων.
2. Στην προσέγγιση αυτο-προσαρμοζόμενου λογισμικού, το λογισμικό στις συσκευές IoT είναι ικανό να ενημερώνεται και να προσαρμόζεται αυτόματα. Μέσω μηχανισμών όπως οι έξυπνοι αλγόριθμοι, το λογισμικό μπορεί να αναγνωρίζει και να αντιμετωπίζει ασφαλείς ενημερώσεις και να εφαρμόζει τις απαιτούμενες διορθώσεις.
3. Η παρακολούθηση της κατάστασης του λογισμικού στις συσκευές IoT είναι σημαντική για την ανίχνευση προβλημάτων και ασφαλείας. Μηχανισμοί παρακολούθησης όπως τα συστήματα ανίχνευσης εισβολών (IDS) μπορούν να εφαρμοστούν για να εντοπίσουν ανωμαλίες και δραστηριότητες που προκαλούν ύποπτες ενέργειες.

2.4.1. Η τεχνική Over-the-Air (OTA)

Η τεχνική Over-the-Air (OTA) αναφέρεται στην ασύρματη μετάδοση δεδομένων ή ενημερώσεων λογισμικού σε ασύρματες συσκευές. Αυτή η τεχνική επιτρέπει την ενημέρωση, αναβάθμιση ή διαχείριση λογισμικού σε απομακρυσμένες συσκευές χωρίς την ανάγκη για φυσική παρέμβαση. Τα κύρια χαρακτηριστικά της τεχνικής OTA περιλαμβάνουν [8]:

- Απομακρυσμένη Ενημέρωση: Η OTA επιτρέπει τη μετάδοση νέων εκδόσεων λογισμικού, παραμέτρων ή διορθώσεων ασφαλείας σε συσκευές απομακρυσμένα, χωρίς την ανάγκη για φυσική παρέμβαση σε κάθε συσκευή ξεχωριστά.
- Ευελιξία: Η OTA επιτρέπει την αναβάθμιση και τη διαχείριση συσκευών απόμακρα, ακόμη και όταν βρίσκονται σε διάφορα γεωγραφικά σημεία.
- Ασφάλεια: Η τεχνική OTA προσφέρει μηχανισμούς ασφαλείας για την ασφαλή μετάδοση και εγκατάσταση των ενημερώσεων λογισμικού, προκειμένου να αποτραπεί η παρείσφρηση και η απειλή της ακεραιότητας του συστήματος.
- Δυνατότητα Επιλεκτικής Ενημέρωσης: Η OTA επιτρέπει την επιλεκτική ενημέρωση συγκεκριμένων συσκευών ή ομάδων συσκευών, ανάλογα με τις ανάγκες και τις προδιαγραφές του διαχειριστή.

2.4.2. Η τεχνική αυτο-προσαρμοζόμενου λογισμικού

Το αυτο-προσαρμοζόμενο λογισμικό αναφέρεται σε μια τεχνική όπου το λογισμικό μπορεί να προσαρμόζεται αυτόματα σε αλλαγές στις συνθήκες λειτουργίας ή στο περιβάλλον. Στο πλαίσιο του IoT, αυτή η τεχνική είναι ιδιαίτερα σημαντική, καθώς οι συσκευές IoT συνήθως λειτουργούν σε διάφορα περιβάλλοντα που αντιμετωπίζουν μεταβαλλόμενες συνθήκες [9]. Οι βασικές χαρακτηριστικές της τεχνικής αυτο-προσαρμοζόμενου λογισμικού στις συσκευές IoT περιλαμβάνουν:

- Αυτόνομη λειτουργία: Οι συσκευές IoT που χρησιμοποιούν αυτο-προσαρμοζόμενο λογισμικό είναι ικανές να προσαρμόζονται αυτόνομα στις μεταβαλλόμενες συνθήκες και απαιτήσεις του περιβάλλοντος τους.
- Ανίχνευση και αξιολόγηση περιβάλλοντος: Οι συσκευές IoT μπορούν να ανιχνεύουν και να αξιολογούν τις μεταβολές στο περιβάλλον τους, όπως αλλαγές στην τοποθεσία, την κίνηση, τη θερμοκρασία κ.λπ
- Αναλογική προσαρμογή: Οι συσκευές IoT μπορούν να προσαρμόζουν τη λειτουργία τους ανάλογα με τις ανιχνευμένες αλλαγές στο περιβάλλον, προσαρμόζοντας την κατανάλωση ενέργειας, την απόδοση ή άλλες παράμετρους.
- Αναδραστικότητα και αυτο-διόρθωση: Οι συσκευές IoT μπορούν να αντιδρούν σε αλλαγές στο περιβάλλον και να προσαρμόζουν τη λειτουργία τους για να διορθώσουν σφάλματα ή να βελτιστοποιήσουν την απόδοσή τους.

2.4.3. Η τεχνική παρακολούθησης της κατάστασης του λογισμικού

Η παρακολούθηση της κατάστασης λογισμικού σε συσκευές IoT αναφέρεται στη διαδικασία παρακολούθησης της ενημερωμένης κατάστασης του λογισμικού που εκτελείται σε μια συσκευή IoT. Αυτό περιλαμβάνει την παρακολούθηση των εκδόσεων του λογισμικού, των διορθώσεων ασφαλείας, των αναβαθμίσεων και άλλων σημαντικών παραμέτρων [10]. Οι τεχνικές παρακολούθησης της κατάστασης λογισμικού σε συσκευές IoT μπορεί να περιλαμβάνουν τα εξής χαρακτηριστικά:

- Επίβλεψη εκδόσεων λογισμικού: Η παρακολούθηση των εκδόσεων του λογισμικού σε μια συσκευή IoT επιτρέπει τον έλεγχο της ενημερωμένης έκδοσης του λογισμικού που εκτελείται σε αυτήν.
- Ενημέρωση λογισμικού: Μέσω της παρακολούθησης της κατάστασης του λογισμικού, μπορεί να πραγματοποιηθεί ενημέρωση του λογισμικού σε μια συσκευή IoT με τη χρήση μηχανισμών όπως η τεχνική Over-the-Air (OTA).
- Διαχείριση διορθώσεων ασφαλείας: Η παρακολούθηση της κατάστασης λογισμικού επιτρέπει την ανίχνευση και την εφαρμογή διορθώσεων ασφαλείας για να αντιμετωπιστούν ευπάθειες και προβλήματα ασφαλείας που μπορεί να επηρεάζουν τη συσκευή IoT.
- Καταγραφή και αναφορά συμβάντων: Η παρακολούθηση της κατάστασης λογισμικού μπορεί να συμπεριλαμβάνει την καταγραφή και αναφορά συμβάντων, όπως σφάλματα, ανωμαλίες και συμπεριφορές που αφορούν το λογισμικό σε μια συσκευή IoT.

2.5. Απομόνωση και εφαρμογή αρχών του ελάχιστου προνομίου

Η απομόνωση και η εφαρμογή των αρχών του ελάχιστου προνομίου (principle of least privilege) σε ένα περιβάλλον IoT είναι σημαντική για τη διασφάλιση της ασφάλειας και της ιδιωτικότητας των δεδομένων. Αυτή η αρχή έχει ως στόχο να περιορίζει τις εξουσιοδοτήσεις και την πρόσβαση των συσκευών και των χρηστών μόνο στις ελάχιστες απαιτούμενες για την εκτέλεση των λειτουργιών τους [7].

Για να εφαρμοστεί η αρχή του ελάχιστου προνομίου σε ένα περιβάλλον IoT, μπορούν να ληφθούν τα εξής μέτρα:

- Αυθεντικοποίηση και εξουσιοδότηση: Κάθε συσκευή IoT πρέπει να αυθεντικοποιείται με μοναδικούς τρόπους, όπως κλειδιά πιστοποίησης ή διαπιστευτήρια χρήστη, προκειμένου να βεβαιωθεί ότι η συσκευή είναι έγκυρη και αξιόπιστη. Επίσης, πρέπει να υπάρχουν μηχανισμοί εξουσιοδότησης για να διασφαλίζεται ότι οι συσκευές έχουν μόνο τις απαιτούμενες εξουσιοδοτήσεις για να εκτελέσουν τις λειτουργίες τους.
- Ελέγχος πρόσβασης και περιορισμοί δικαιωμάτων: Οι προνομιούχοι χρήστες ή συσκευές IoT πρέπει να έχουν μόνο τα απαραίτητα δικαιώματα για να εκτελέσουν τις απαιτούμενες λειτουργίες. Αυτό προστατεύει το σύστημα από εκμεταλλεύσεις ευπαθειών ή ανεξέλεγκτες προσπάθειες πρόσβασης.
- Κατάτμηση και απομόνωση: Οι συσκευές IoT πρέπει να κατατμηθούν σε λειτουργικές μονάδες και να απομονωθούν μεταξύ τους. Αυτό μπορεί να επιτευχθεί με τη χρήση ανεξάρτητων επιπέδων λογισμικού ή εικονικών μηχανών για κάθε συσκευή. Αυτός ο διαχωρισμός μειώνει τον κίνδυνο εξάπλωσης επιθέσεων και περιορίζει τον αντίκτυπο πιθανών ευπαθειών.

2.5.1. Αυθεντικοποίηση και εξουσιοδότηση

Η αυθεντικοποίηση και η εξουσιοδότηση είναι δύο σημαντικές διαδικασίες στο πλαίσιο της ασφάλειας των συσκευών IoT. Αναφέρονται στην επιβεβαίωση της ταυτότητας και των δικαιωμάτων μιας συσκευής πριν την αποδοχή της και την παροχή πρόσβασης σε πόρους ή λειτουργίες. [11]

- Η αυθεντικοποίηση στοχεύει στη διασφάλιση ότι μια συσκευή IoT είναι πραγματικά αυτή που ισχυρίζεται να είναι και ότι δεν έχει τροποποιηθεί ή παραβιαστεί. Αυτό επιτυγχάνεται μέσω μηχανισμών όπως οι κρυπτογραφικές υπογραφές, τα πιστοποιητικά και οι κλειδώσεις πρόσβασης. Κατά τη διαδικασία αυθεντικοποίησης, η συσκευή προσκομίζει δεδομένα για την ταυτότητά της, όπως πιστοποιητικά ή κλειδιά.
- Η εξουσιοδότηση αναφέρεται στην απόφαση ή την απόδοση προνομίων σε μια συσκευή μετά την αυθεντικοποίηση. Αυτό περιλαμβάνει την αξιολόγηση των δικαιωμάτων και των προνομίων της

συσκευής και την παροχή πρόσβασης μόνο σε εκείνους τους πόρους ή τις λειτουργίες που της επιτρέπονται.

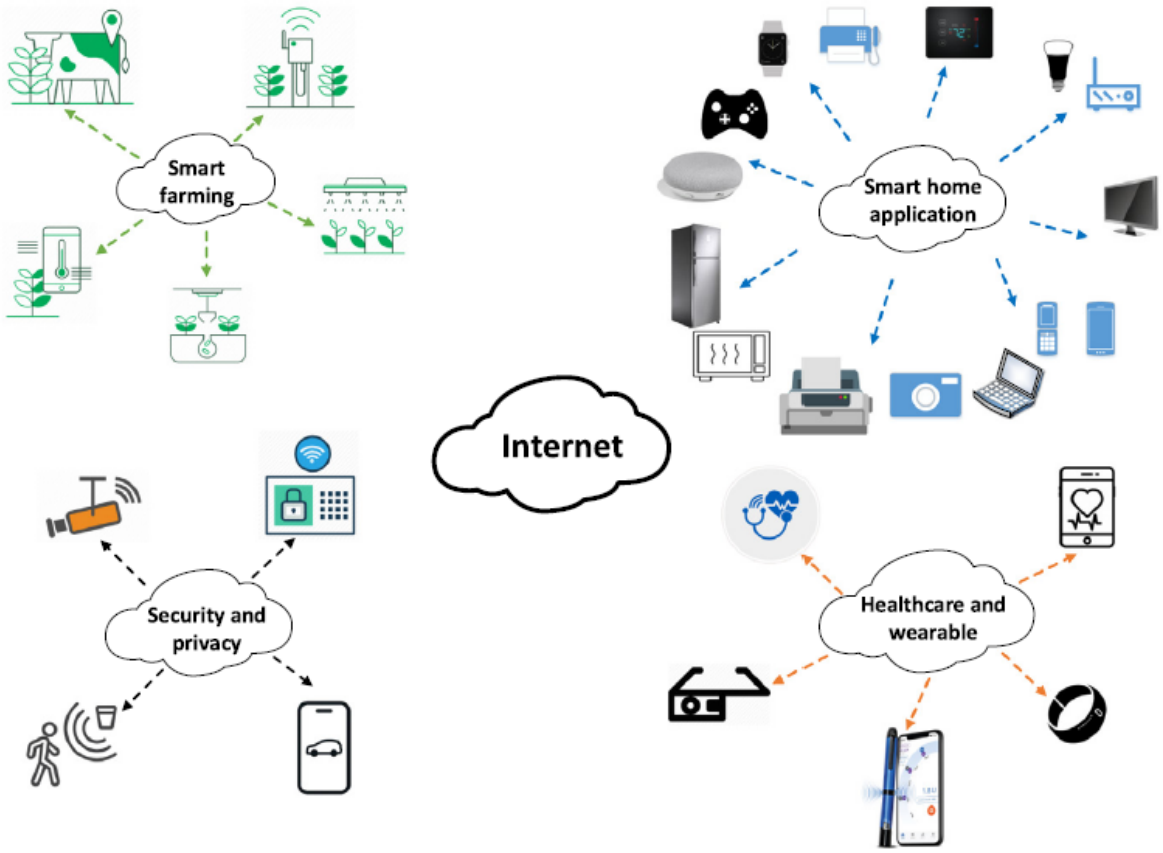
2.5.2. Κατάτμηση και απομόνωση

Η κατάτμηση και η απομόνωση είναι δύο βασικές ασφαλείς αρχές που εφαρμόζονται σε συσκευές IoT για την προστασία τους από επιθέσεις και κακόβουλες ενέργειες.

- Κατάτμηση (Segmentation) αναφέρεται στον διαχωρισμό της συσκευής IoT σε λογικές ή φυσικές ομάδες, με σκοπό να περιοριστεί η επικοινωνία και οι πρόσβαση σε ευαίσθητα στοιχεία και λειτουργίες. Αυτό γίνεται για να μειωθεί ο κίνδυνος διάδοσης επιθέσεων και η επίδρασή τους σε άλλα μέρη του συστήματος. Με την κατάτμηση, οι συσκευές IoT διαιρούνται σε διακριτές ζώνες ή τομείς (zones) με βάση τη λειτουργία, την τοποθεσία, τον τύπο των δεδομένων και άλλους παράγοντες. Αυτή η διάκριση μπορεί να γίνει σε επίπεδο δικτύου, λειτουργικού συστήματος ή εφαρμογής.
- Απομόνωση (Isolation) σημαίνει την απομάκρυνση και περιορισμό των πόρων και των δυνατοτήτων των συσκευών IoT, προκειμένου να περιοριστεί η πιθανότητα ανεπιθύμητων ενεργειών ή πρόσβασης. Αυτό σημαίνει ότι η κάθε συσκευή έχει περιορισμένες αρμοδιότητες και δικαιώματα πρόσβασης, και μπορεί να αλληλοεπιδράσει μόνο με επιλεγμένους πόρους και άλλες συσκευές που είναι απαραίτητες για τη λειτουργία της. Αυτό επιτυγχάνεται με τη χρήση μηχανισμών περιορισμένων δικαιωμάτων, όπως ρόλους και αδειοδοτήσεις (licensing).

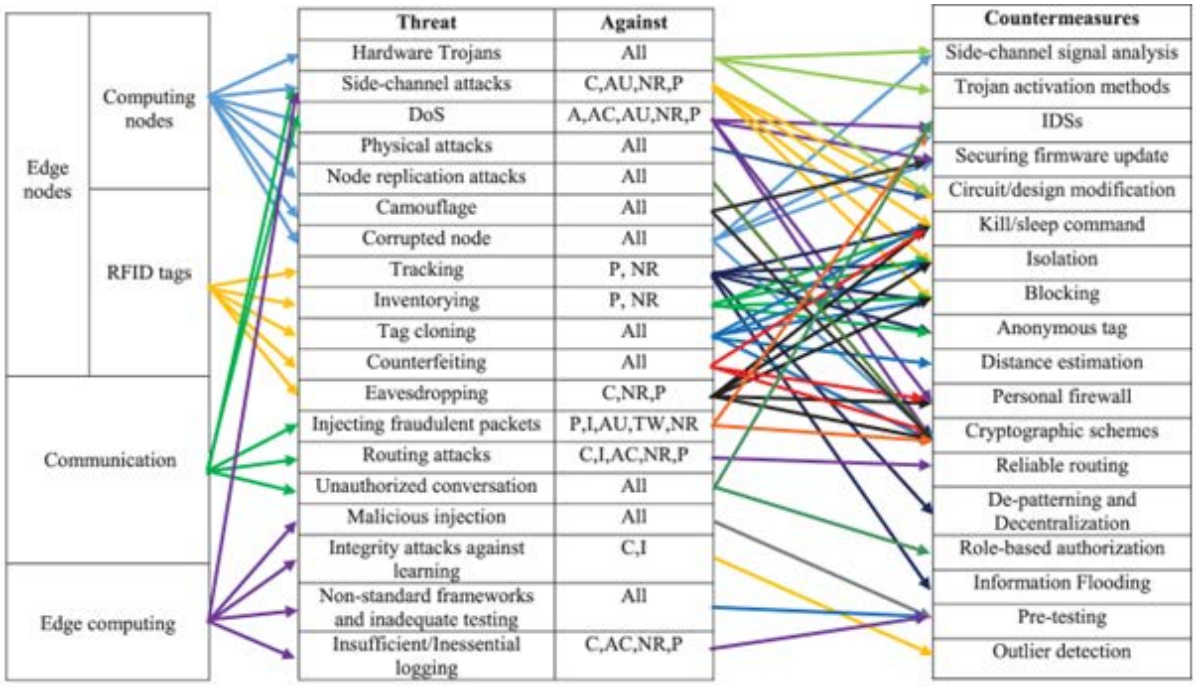
3ο ΚΕΦΑΛΑΙΟ: ΑΝΑΓΚΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IOT

Υπάρχουν διάφοροι παράγοντες που συμβάλλουν στην τεράστια ευπάθεια ασφαλείας των IoT, συμπεριλαμβανομένης της περιορισμένης διαθέσιμης ενέργειας στους κόμβους IoT, της χαμηλής υπολογιστικής τους ικανότητας, των πολλαπλών ετερογενών διασυνδέσεων σε ένα δίκτυο καθώς και της ετερογενούς φύσης του δικτύου [12]. Αυτά τα χαρακτηριστικά, ιδίως ο αριθμός των συνδεδεμένων συσκευών, συχνά οδηγούν σε αναποτελεσματική απόδοση των συμβατικών μηχανισμών ασφαλείας. Αυτές οι συσκευές πρέπει να μεταδίδουν τα δεδομένα που συνέλεξαν και να αντιδρούν στις πληροφορίες που λαμβάνουν.



Σχήμα 2 Παραδείγματα εφαρμογών και τοπολογιών IoT [50].

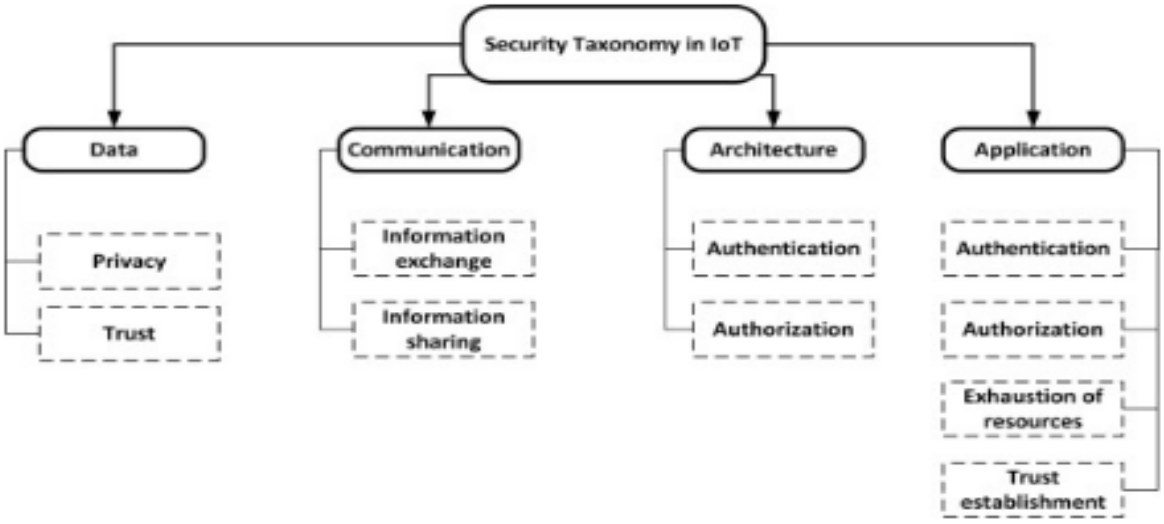
Η εμπορευματοποίηση του IoT έχει οδηγήσει σε ανησυχίες για τη δημόσια ασφάλεια, συμπεριλαμβανομένων ζητημάτων προσωπικού απορρήτου, απειλών επιθέσεων στον κυβερνοχώρο και οργανωμένου εγκλήματος. Μια ολοκληρωμένη λίστα τρωτών σημείων και αντίμετρων εναντίον τους στο επίπεδο του IoT παρατίθεται ακολούθως [27]:



Requirement	Definition	Abbreviations
Confidentiality	Ensuring that only authorized users access the information	C
Integrity	Ensuring completeness, accuracy, and absence of unauthorized data manipulation	I
Availability	Ensuring that all system services are available, when requested by an authorized user	A
Accountability	An ability of a system to hold users responsible for their actions	AC
Auditability	An ability of a system to conduct persistent monitoring of all actions	AU
Trustworthiness	An ability of a system to verify identity and establish trust in a third party	TW
Non-repudiation	An ability of a system to confirm occurrence/non-occurrence of an action	NR
Privacy	Ensuring that the system obeys privacy policies and enabling individuals to control their personal information	P

Σχήμα 3 Τα τρία επίπεδα του δικτυακού νέφους: (i) ακραίοι κόμβοι, (ii) επικοινωνία και (iii) ακραίοι υπολογιστικοί κόμβοι.

Οι διάφορες έννοιες ασφάλειας για το IoT διακρίνονται σε τέσσερις τομείς με βάση τη βιβλιογραφία [16], [17], [18] και παρουσιάζονται στο Σχήμα 2.



Σχήμα 4 Οι διάφορες έννοιες ασφάλειας για το IoT διακεκριμένες σε τομείς [50].

Οι προκλήσεις ασφαλείας στα IoT μπορούν να ταξινομηθούν ευρέως στις ακόλουθες:

1. αναγνώριση,
2. έλεγχο ταυτότητας,
3. κρυπτογράφηση,
4. εμπιστευτικότητα,
5. παρεμβολή,
6. κλωνοποίηση,
7. διείσδυση, και
8. ιδιωτικότητα.

3.1. Αναγνώριση

Με βάση το επίπεδο πρόσβασης στο δίκτυο, αυτοί οι τύποι επιθέσεων κατηγοριοποιούνται σε δύο διαφορετικούς κλάδους και συγκεκριμένα, τις παθητικές και τις ενεργητικές επιθέσεις.

- Στις περισσότερες παθητικές επιθέσεις, ο εισβολέας απλώς κρυφακούει την επικοινωνία μεταξύ του νόμιμου πομπού και του δέκτη του για να εκμεταλλευτεί τα δεδομένα τους [19], [20].
- Στις ενεργές επιθέσεις, ο εισβολέας επιχειρεί να διαταράξει τη σύνδεση μεταξύ των νόμιμων οντοτήτων, να πραγματοποιήσει ο ίδιος πλαστοπροσωπία ή ακόμα και να διακόψει τη σύνδεση χειραγωγώντας τις πληροφορίες δρομολόγησης [19], [21], [22].

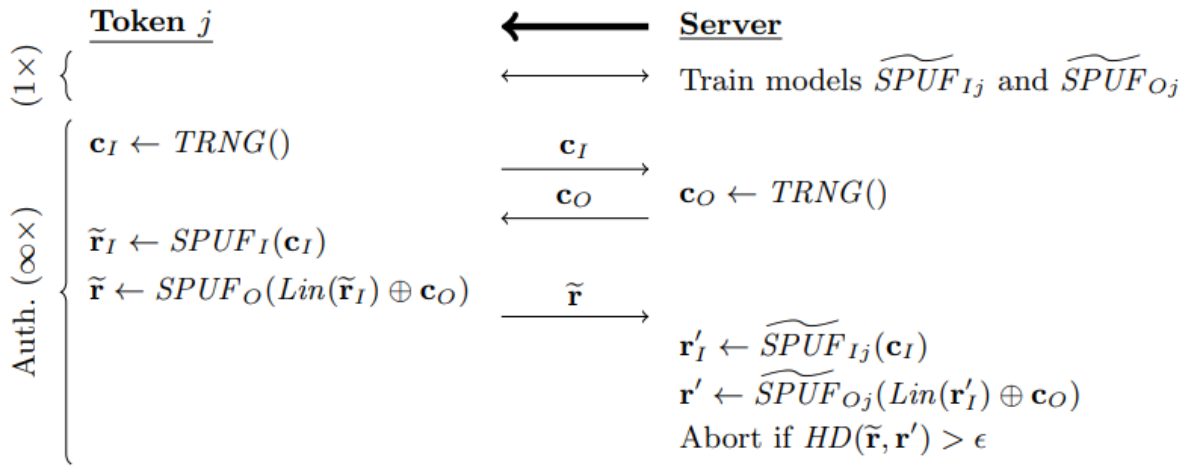
Επίσης, με βάση το προφίλ των IoT συσκευών (υψηλού και χαμηλού επιπέδου), οι επιθέσεις ενδέχεται απλώς να οδηγήσουν σε μη φυσιολογική συμπεριφορά ή να σταματήσουν τη λειτουργία των συσκευών [19].

- Στην κατηγορία προφίλ υψηλού επιπέδου χρησιμοποιείται η υπολογιστική ισχύ των CPU και ακόμη και των GPU και η δικτυακή σύνδεση για να εξαπολύσουν επιθέσεις στο δίκτυο IoT [23], [24].
- Στην κατηγορία προφίλ χαμηλού επιπέδου συσκευές που έχουν χαμηλή ισχύ και ενέργεια εμπλέκονται σε επιθέσεις σε συσκευές IoT, όπως για παράδειγμα τα έξυπνα ρολόγια ή τα έξυπνα οικιακά gadgets. Χρησιμοποιεί την ασύρματη σύνδεση μεταξύ του και της συσκευής IoT για να εκτελέσει την επίθεση [25], [26].

3.2. Έλεγχος ταυτότητας

Η έρευνα για πρωτόκολλα ελέγχου ταυτότητας (authentication) που χρησιμοποιούνται σε PUF που προτάθηκαν μεταξύ 2001 και 2014 αποκαλύπτει διαφορετικά ζητήματα ασφάλειας σε αυτά [27]. Η

συμπεριφορά εισόδου-εξόδου του PUF είναι ένα βασικό συστατικό του ίδιου του πρωτοκόλλου. Για κάθε διακριτικό j, ο διακομιστής συλλέγει αυθαίρετα δεδομένα ως πρόκληση. Ένα γνήσιο διακριτικό ταυτότητας θα πρέπει να μπορεί να αναπαράγει την απάντηση για κάθε πρόκληση στη βάση δεδομένων του διακομιστή. Απαιτείται μόνο μια κατά προσέγγιση αντιστοίχιση, λαμβάνοντας υπόψη ο θόρυβος PUF αντιμετωπίζεται με μηχανισμό ανίχνευσης και διόρθωσης σφάλματος ψηφίου κατά Hamming. Για την αποφυγή πλαστοπροσωπίας μέσω επανάληψης μηνυμάτων, οι προκλήσεις απορρίπτονται μετά τη χρήση, περιορίζοντας τον αριθμό των ελέγχων ταυτότητας. Παρόλα αυτά, ένας εισβολέας μπορεί να εκτελέσει άρνηση υπηρεσίας μέσω εξάντλησης της βάσης δεδομένων διακομιστή.



Σχήμα 5 Μηχανισμός ελέγχου ταυτότητας βασισμένος σε βασικό PUF [27].

Οι PUF μπορούν να χρησιμοποιηθούν σε διάφορα πρωτόκολλα ελέγχου ταυτότητας. Ορισμένα από αυτά τα ζητήματα περιλαμβάνουν:

- Αντιστοίχιση μοναδικής ταυτότητας: Ένα ισχυρό PUF πρέπει να μπορεί να παράγει μια μοναδική ταυτότητα για κάθε συσκευή. Η διαδικασία αντιστοίχισης της ταυτότητας πρέπει να είναι ασφαλής και απαραβίαστη.
- Προστασία των κλειδιών: Τα κλειδιά που χρησιμοποιούνται για την επαλήθευση της ταυτότητας πρέπει να προστατεύονται από ανεπιθύμητη πρόσβαση. Αυτό μπορεί να επιτευχθεί μέσω μηχανισμών κρυπτογράφησης και αποθήκευσης κλειδιών σε ασφαλή στοιχεία του συστήματος.
- Προστασία από επιθέσεις εξαντλητικής αναζήτησης: Οι προστατευτικοί μηχανισμοί πρέπει να εφαρμοστούν για να περιορίσουν τον αριθμό των δοκιμών που μπορούν να γίνουν κατά την επαλήθευση της ταυτότητας.
- Αποτροπή επιθέσεων μεσάζοντα (man-in-the-middle attacks): Οι πρωτόκολλα ελέγχου ταυτότητας πρέπει να παρέχουν μηχανισμούς για την ανίχνευση και αποτροπή αυτών των επιθέσεων.

3.3. Κρυπτογράφηση

Οι προκλήσεις ασφάλειας και απορρήτου σε περιβάλλον IoT γενικά και οι πιθανές επιθέσεις σε διαφορετικά επίπεδα συσκευών IoT σε περιβάλλον cloud/edge είναι πολλές [28]. Ορισμένες από τις κύριες προκλήσεις ασφάλειας και απορρήτου του IoT περιλαμβάνουν:

- Με την αύξηση του αριθμού των συνδεδεμένων συσκευών IoT, αυξάνεται και η επιθυμία για εισβολή στο δίκτυο και την παρακολούθηση των συσκευών αυτών.
- Υπάρχει έλλειψη παγκόσμιων προτύπων ασφάλειας για τις συσκευές IoT, πράγμα που δυσκολεύει την ανάπτυξη κοινών μεθόδων προστασίας και εκθέτει το δίκτυο σε ευπάθειες.
- Ορισμένες συσκευές IoT δεν υποστηρίζουν ενημερώσεις λογισμικού και κατά συνέπεια είναι αδύνατη αναβάθμιση των συσκευών. Επομένως, αν ανακαλυφθεί μια αδυναμία ασφάλειας σε αυτές τις συσκευές, είναι δύσκολο να επιλυθεί.
- Η αναγνώριση των συσκευών IoT και η πιστοποίηση της ταυτότητάς τους είναι μια πρόκληση, καθώς οι συσκευές μπορεί να χρησιμοποιούνται από ανεπιθύμητους χρήστες ή να υποκλαπούν οι πιστοποιητικές αρχές.

Όσον αφορά τις πιθανές επιθέσεις σε διαφορετικά επίπεδα συσκευών IoT, ορισμένες από τις κύριες είναι:

- Φυσικό Επίπεδο: Επιθέσεις όπως η καταστροφή των φυσικών συσκευών ή η παρεμπόδιση των ασύρματων σημάτων μπορούν να προκαλέσουν διακοπή της λειτουργίας των συσκευών.
- Επίπεδο δικτύου: Επιθέσεις όπως η διάρρηξη του δικτύου, η καταστροφή ή η παρεμπόδιση των μηνυμάτων επικοινωνίας μπορούν να παρεμποδίσουν την αποτελεσματική λειτουργία του IoT.
- Επίπεδο εφαρμογών: Επιθέσεις όπως η παρείσφρηση σε εφαρμογές IoT μπορούν να οδηγήσουν στην παραβίαση των προσωπικών δεδομένων ή την αποκάλυψη ευαίσθητων πληροφοριών.
- Επίπεδο διαχείρισης: Επιθέσεις όπως η υποκλοπή διαπιστευτηρίων διαχείρισης, η κακόβουλη αλλαγή των ρυθμίσεων ή η παραβίαση των μηχανισμών ενημέρωσης μπορούν να οδηγήσουν σε ανεπιθύμητο έλεγχο των συσκευών IoT.

Στο [46] συζητήθηκαν οι αδυναμίες ασφάλειας του IoT σε διαφορετικά επίπεδα επικοινωνίας, όπως ενδεικτικά παρουσιάζονται ακολούθως:

Security mode	Security provided
No Security	Data is not encrypted Data authenticity is not validated
AES-CBC-MAC-32	Data is not encrypted Data authenticity using a 32-bit MIC
AES-CBC-MAC-64	Data is not encrypted Data authenticity using a 64-bit MIC
AES-CBC-MAC-128	Data is not encrypted Data authenticity using a 128-bit MIC
AES-CTR	Data is encrypted Data authenticity is not validated
AES-CCM-32	Data is encrypted Data authenticity using a 32-bit MIC
AES-CCM-64	Data is encrypted Data authenticity using a 64-bit MIC
AES-CCM-128	Data is encrypted Data authenticity using a 128-bit MIC

Σχήμα 6 Σχήματα ασφαλείας επικοινωνιών πρωτοκόλλου IEEE 802.15.4 [46].

3.4. Εμπιστευτικότητα

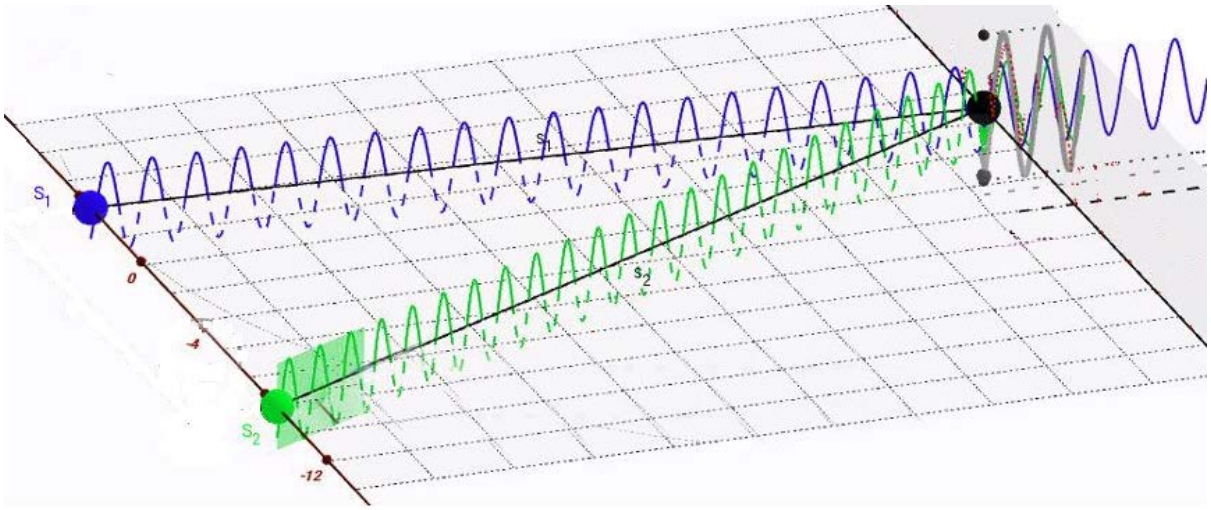
Οι μέθοδοι κρυπτογράφησης είναι ένα κρίσιμο στοιχείο για την ασφάλεια των συστημάτων IoT. Θεωρητικά, η κρυπτογράφηση μηνυμάτων δεν επιτρέπει στους χάκερ να έχουν πρόσβαση στα μηνύματα και εξαλείφει τον κίνδυνο χειραγώγησης δεδομένων. Ωστόσο, η κρυπτογράφηση από μόνη της δεν παρέχει ούτε εγγυάται την ακεραιότητα. Για παράδειγμα, ένα κρυπτογραφημένο μήνυμα μπορεί ακόμα να αποκρυπτογραφηθεί, αλλά το αποτέλεσμα δεν είναι πλήρως σαφές. Επιπλέον, η κρυπτογράφηση από μόνη της δεν μπορεί να αποτρέψει κακόβουλα τρίτα μέρη από τη μετάδοση κρυπτογραφημένων πακέτων στο δίκτυο.

Αρκετοί ευρέως χρησιμοποιούμενοι μηχανισμοί κρυπτογράφησης, όπως η υποδομή δημόσιου κλειδιού (PKI), το προηγμένο πρότυπο κρυπτογράφησης (AES) και η κρυπτογραφία ελλειπτικής καμπύλης (ECC) βασίζονται σε μυστικά κλειδιά. Τα κρυπτογραφικά κλειδιά είναι ευαίσθητες πληροφορίες και ως εκ τούτου, έχουν αναπτυχθεί αρκετοί μηχανισμοί για την προστασία αυτών των κλειδιών. Η διαχείριση κλειδιών σε ένα δίκτυο IoT είναι ακόμη πιο δύσκολη λόγω του αυξανόμενου αριθμού συσκευών. Η διαδικασία παραγωγής, διανομής και αποθήκευσης κλειδιών σε μεγάλης κλίμακας δίκτυα IoT εξακολουθεί να αποτελεί σημαντική πρόκληση για την ασφάλεια του IoT.

3.5. Παρεμβολή

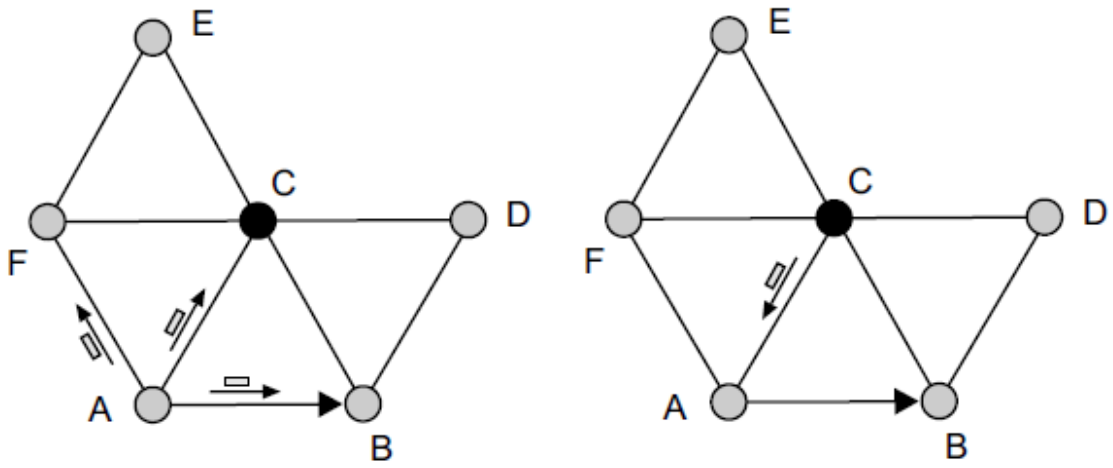
Οι λειτουργίες επικοινωνίας των δικτύων IoT περιγράφονται συνήθως από το μοντέλο TCP/IP.

- Στο φυσικό επίπεδο η παρεμβολή γίνεται με ραδιοεκπομπές [29].

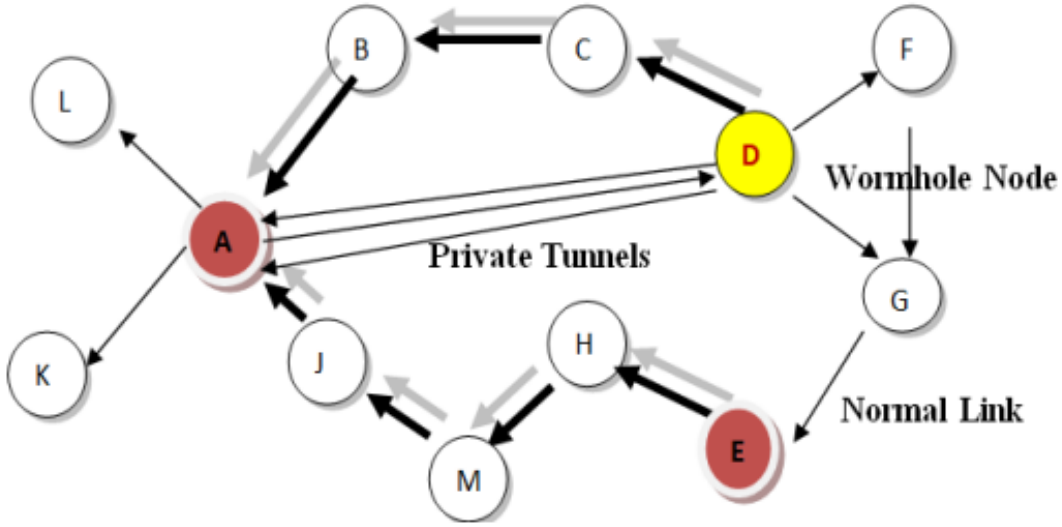


Σχήμα 7 Παρεμβολή με ραδιοεκπομπή από τρίτη πηγή.

- Στο επίπεδο σύνδεσης δεδομένων η παρεμβολή γίνεται (α) με συγκρούσεις μέσω της ταυτόχρονης μετάδοσης δεδομένων στο ίδιο κανάλι [30], (β) με εξάντληση των πόρων λόγο πολλαπλών συγκρούσεων και συνεχών αναμεταδόσεων [31], και (γ) με μέσο της επίμονης, επανειλημμένης ζήτησης πόρων από το κανάλι με αποτέλεσμα να περιορίσει ή και να αποκλείσει κάθε άλλο αίτημα [32].
- Στο επίπεδο δικτύου (α) η επιλεκτική προώθηση μέσω της αποστολής επιλεγμένων πληροφοριών στον νόμιμο παραλήπτη [33], (β) η μετατροπή ενός κόμβου σε στόχο όλων των άλλων για συλλογή πληροφοριών (SinkHole) [34] (γ) με την πλαστή επιβεβαίωση επιπέδου σύνδεσης [35], (δ) με την πλημύρα του καναλιού με μηνύματα Hello [36], και (ε) με την αναμετάδοση δεδομένων στους κόμβους IoT (WormHoles) [37].

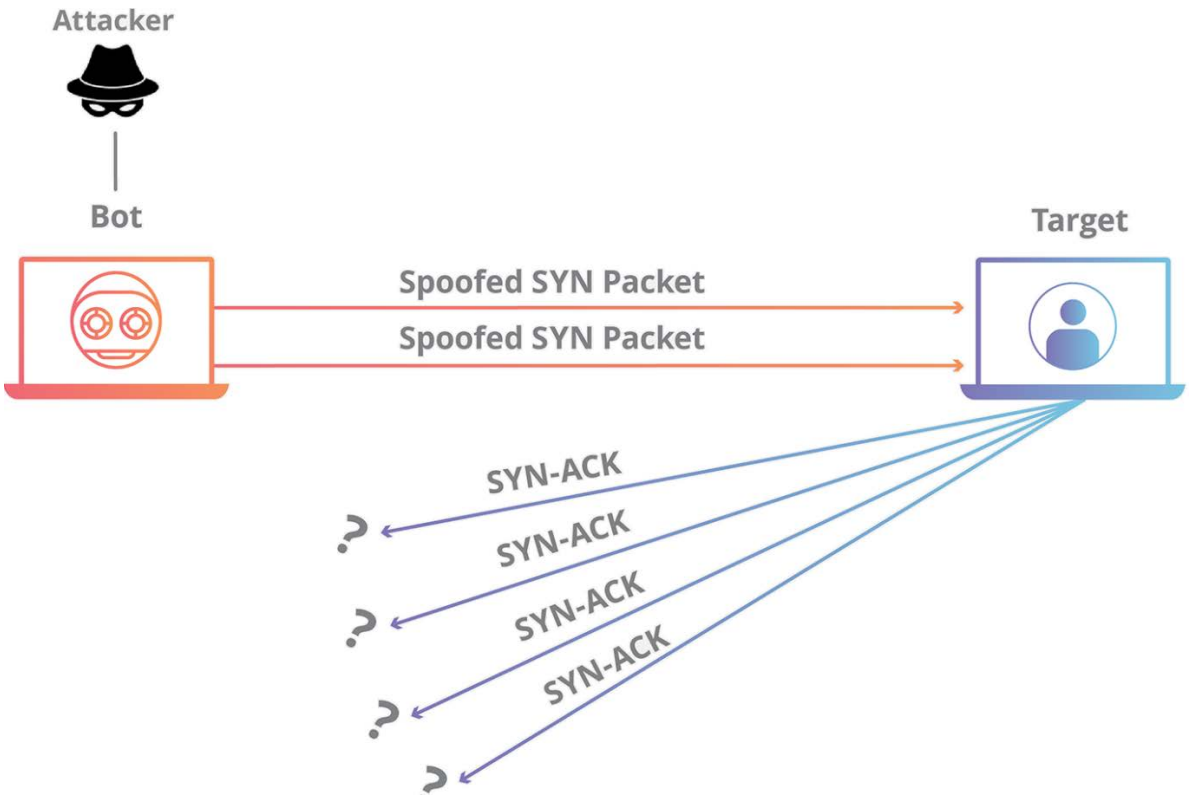


Σχήμα 8 Επίθεση SinkHole [34] (ο κόμβος C συμπεριφέρεται ως ο B).

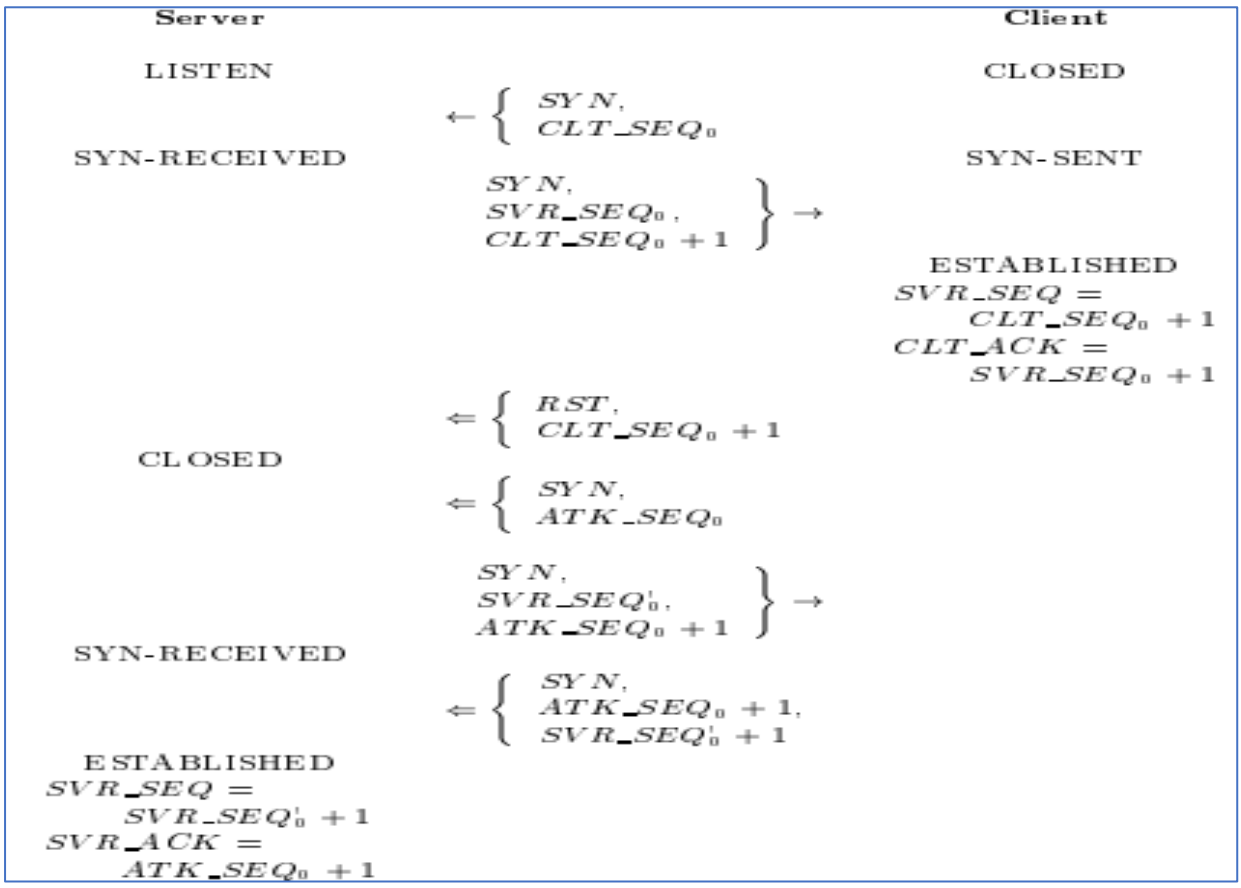


Σχήμα 9 Επίθεση WormHole [37] (δημιουργούνται τούνελ μεταξύ των κόμβων).

- Στο επίπεδο δικτύου (α) με την αναμετάδοση μηνύματος SYN μέχρι πλήρωσης της χωρητικότητας του καναλιού (SYN flooding) [38], και (β) με την επαναρχικοποίηση της σύνδεσης με αποτέλεσμα τον αποσυγχρονισμό της [39].



Σχήμα 10 Επίθεση Syn Flooding [38]

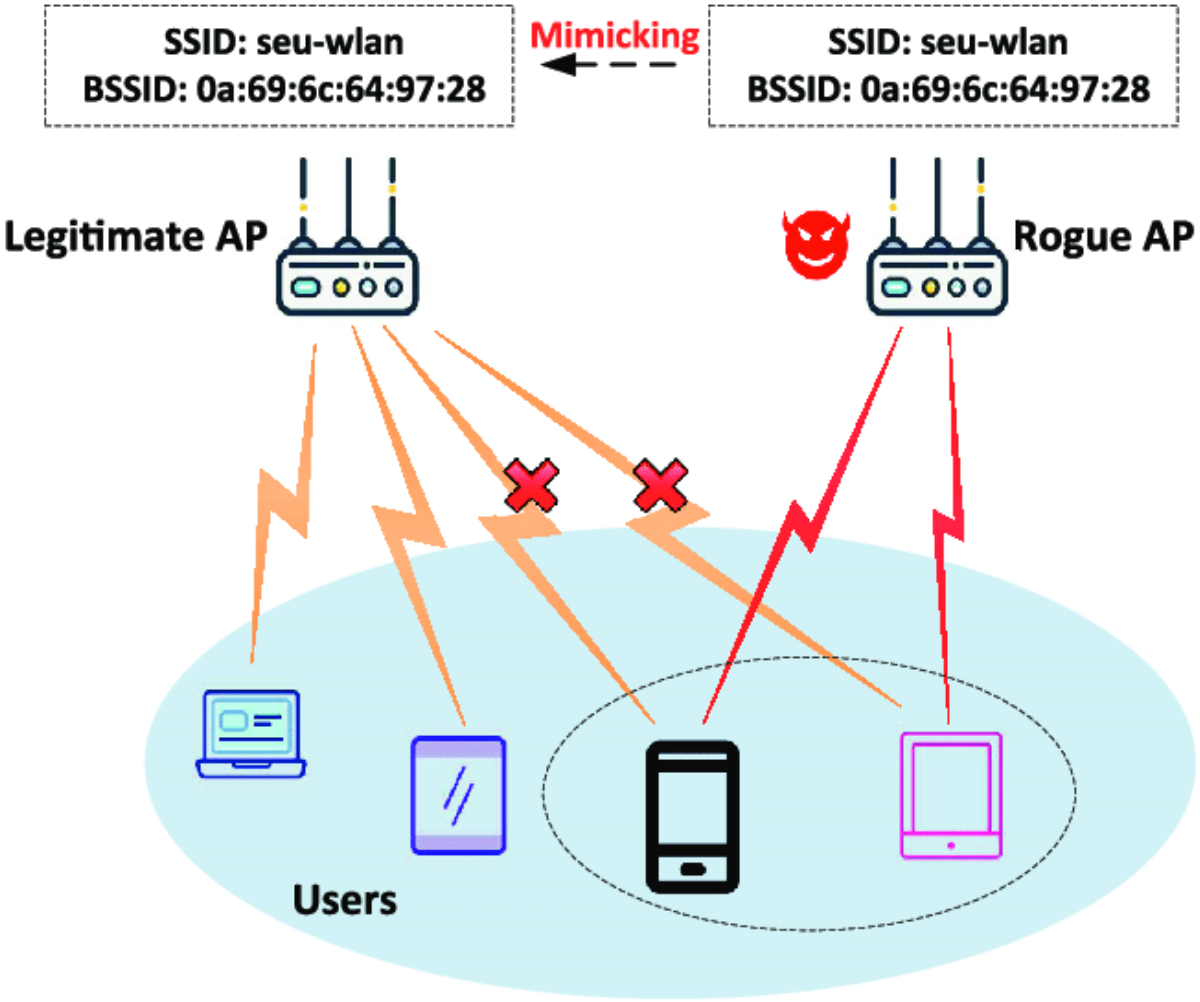


Σχήμα 11 Επίθεση επαναρχικοποίησης (οι επιθέσεις σημειώνονται με <=) [39]

- Στο επίπεδο εφαρμογής με επιθέσεις αξιοπιστίας εφαρμογής, παραμόρφωση της συγκέντρωσης δεδομένων, επιλεκτικό μήνυμα, προώθηση, και στρεβλώσεις του ρολογιού [40].

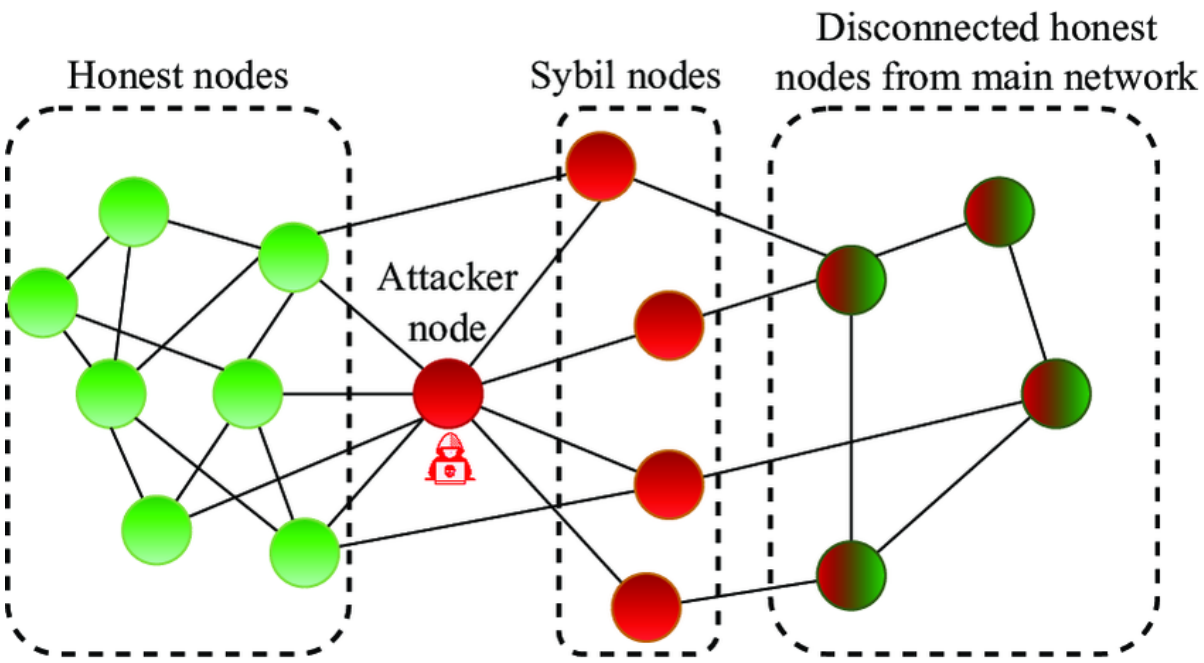
3.6. Κλωνοποίηση

- Στο φυσικό επίπεδο η παραβίαση [41] με δημιουργία ψευδεπίγραφων κόμβων



Σχήμα 12 Επίθεση ψευδεπίγραφου κόμβου (σημείο πρόσβασης) [41]

- Στο επίπεδο δικτύου (α) η πλαστογράφηση του δικτύου ή επανάληψη πληροφοριών δρομολόγησης [42], (β) με την δημιουργία πολλαπλών ψευδώνυμων ταυτοτήτων για την αποδιοργάνωση του εξουσιοδοτημένου συστήματος (Sybil) [43].



Σχήμα 13 Επίθεση Sybil [43].

3.7. Διείσδυση

Οι προκλήσεις ασφάλειας σε συνδέσεις IoT είναι πολύ σημαντικές λόγω της μεγάλης αποκέντρωσης και του μεγάλου αριθμού συνδεδεμένων συσκευών. Ορισμένα ζητήματα ασφάλειας που σχετίζονται με τις διεισδύσεις στα συστήματα IoT περιλαμβάνουν:

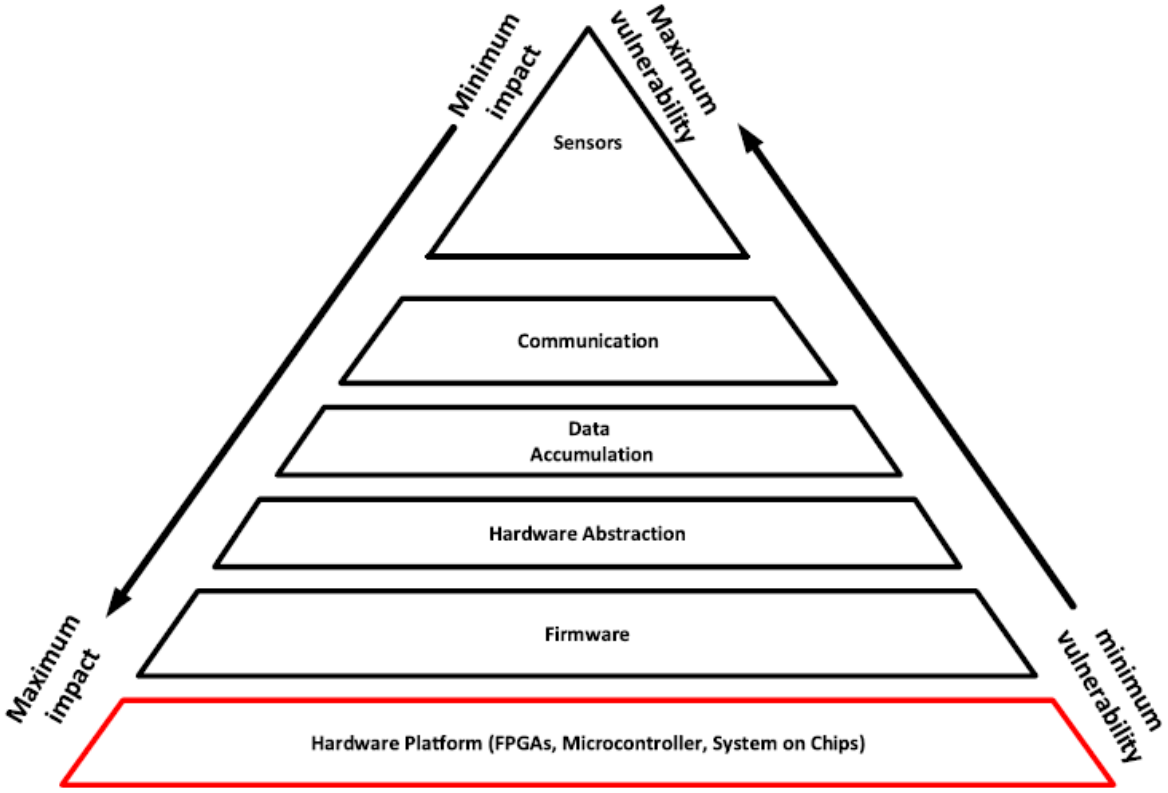
- Αδύναμες εργοστασιακές προεπιλογές: Οι περισσότερες συσκευές IoT παραδίδονται με προεπιλεγμένες διαπιστευτήρια πρόσβασης (π.χ. όνομα χρήστη και κωδικός πρόσβασης) που είναι ευρέως γνωστά ή εύκολα επιλέξιμα. Αυτό καθιστά εύκολη τη διείσδυση στις συσκευές IoT, ειδικά εάν δεν αλλάξουν αυτές οι προεπιλεγμένες ρυθμίσεις από τους χρήστες.
- Μη ασφαλείς συνδέσεις: Οι ασφάλεια των συνδέσεων μεταξύ των συσκευών IoT, των πύλων και των απομακρυσμένων συστημάτων είναι κρίσιμη. Αν οι συνδέσεις δεν είναι ασφαλείς, οι επιτιθέμενοι μπορούν να παρακολουθήσουν και να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα.
- Αδύναμα πρωτόκολλα επικοινωνίας: Ορισμένα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στα συστήματα IoT μπορεί να παρουσιάζουν αδυναμίες ασφαλείας. Αυτό μπορεί να επιτρέψει σε επιτιθέμενους να χρησιμοποιήσουν ευπάθειες των πρωτοκόλλων για να πραγματοποιήσουν επιθέσεις όπως την ψευδο-επαλήθευση (spoofing) ή την αποκάλυψη δεδομένων.
- Ελλιπής διαχείριση και ενημέρωση: Η έλλειψη συστηματικής διαχείρισης και ενημέρωσης των συσκευών IoT μπορεί να αποτελέσει μια αδυναμία ασφαλείας. Αν δεν εγκατασταθούν ενημερώσεις ασφαλείας ή αν δεν διαχειριστούν οι αδυναμίες ασφαλείας, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν τις ευπάθειες για να αποκτήσουν πρόσβαση.

3.8. Ιδιωτικότητα

Στο [44], συζητήθηκαν οι προκλήσεις ασφάλειας και απορρήτου του IoT γενικά και πιθανές επιθέσεις σε διαφορετικά επίπεδα συσκευών IoT. Ειδικότερα, η αναφερόμενη εργασία συζητά τις προκλήσεις ασφαλείας του IoT που βασίζεται σε υπολογιστές ομίχλης/άκρου. Στο [45], εισήχθη η χρήση της πληροφοριοκεντρικής δικτύωσης (ICN) ως πιθανό πρωτόκολλο για την αντιμετώπιση συσκευών IoT όσον αφορά την προσωρινή αποθήκευση εντός του δικτύου, τα σχήματα ονομασίας περιεχομένου, τα σχήματα ασφαλείας και τα σχήματα χειρισμού κινητικότητας. Οι συντάκτες του [44] τονίζουν την ανάγκη για «μεγαλύτερο και μόνιμο σχήμα ονοματοδοσίας και χώρο διευθύνσεων για περιεχόμενο και συσκευές IoT» [45]. Στο [46], οι συγγραφείς εστίασαν στην ασφάλεια των επικοινωνιών μεταξύ συσκευών IoT χρησιμοποιώντας διαφορετικά πρωτόκολλα και μηχανισμούς και συζητήθηκαν επίσης οι αδυναμίες ασφάλειας του IoT σε διαφορετικά επίπεδα επικοινωνίας. Στο [47], οι συγγραφείς συζήτησαν τη χρήση προγραμματιζόμενου υλικού όπως τα FPGA στην ασφάλεια της υποδομής δικτύου. Ο συγγραφέας τόνισε το ρόλο των μηχανισμών που βασίζονται σε υλικό για την αντιμετώπιση ορισμένων από τις προκλήσεις στις μεθόδους που βασίζονται σε λογισμικό, καθώς και τις πιθανές προκλήσεις λόγω των αυξανόμενων απαιτήσεων για εντατική ανάλυση και λειτουργία σε πραγματικό χρόνο για διαδοχική επεξεργασία.

4ο ΚΕΦΑΛΑΙΟ: ΠΡΑΚΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ

Η αντιμετώπιση των απειλών ασφαλείας απαιτεί την ιεράρχηση της απειλής. Η ιεράρχηση βασίζεται στην αποτίμηση των επιπτώσεων της επέλευσης της σε συνδυασμό με την πιθανότητα επέλευσης της, όπως περιγράφει το ακόλουθο Σχήμα 3.



Σχήμα 14 Πυραμίδα αποτίμησης κινδύνου IoT περιβάλλοντος [50].

Γενικά, υπάρχουν δύο τύποι μηχανισμών που βασίζονται σε λογισμικό και βασισμένοι σε υλικό για την προστασία των συσκευών IoT από διάφορες επιθέσεις:

- Οι μηχανισμοί ασφαλείας που βασίζονται σε λογισμικό βασίζονται αποκλειστικά σε λογισμικό για την προστασία των μηνυμάτων τους. Βασίζονται σε μαθηματικές προσεγγίσεις (π.χ. ένα διακριτό λογαριθμικό πρόβλημα) που μπορεί να μην είναι εύκολα επιλύσιμα χρησιμοποιώντας τους σημερινούς υπολογιστές, αλλά όταν η ύπαρξη κβαντικών υπολογιστών γίνει πραγματικότητα, μπορούν να λυθούν σε συντομότερο χρόνο σε σύγκριση με τις παραδοσιακές μεθόδους για εξαγωγή των κλειδιών [33]. Επιπλέον, σε μηχανισμούς ασφαλείας που βασίζονται σε λογισμικό, τα κλειδιά αποθηκεύονται στην προσωρινή μνήμη NVM των συσκευών που είναι επιρρεπείς σε επιθέσεις. Αν και τα συστήματα ασφαλείας που βασίζονται σε λογισμικό ήταν αποτελεσματικά όλα αυτά τα χρόνια, η πρόοδος στο υλικό και τους υπολογιστές μπορεί να επιτρέψει στους χάκερ να τα σπάσουν χρησιμοποιώντας κβαντικούς υπολογιστές [48]. Καθώς διατίθενται πολλοί πόροι για τη δημιουργία κβαντικών υπολογιστών, η ύπαρξή τους θα γίνει σύντομα πραγματικότητα. Επομένως,

όλοι οι υπάρχοντες μηχανισμοί ασφάλειας λογισμικού διατρέχουν υψηλό κίνδυνο, γεγονός που απαιτεί πρόσθετες λύσεις ασφάλειας.

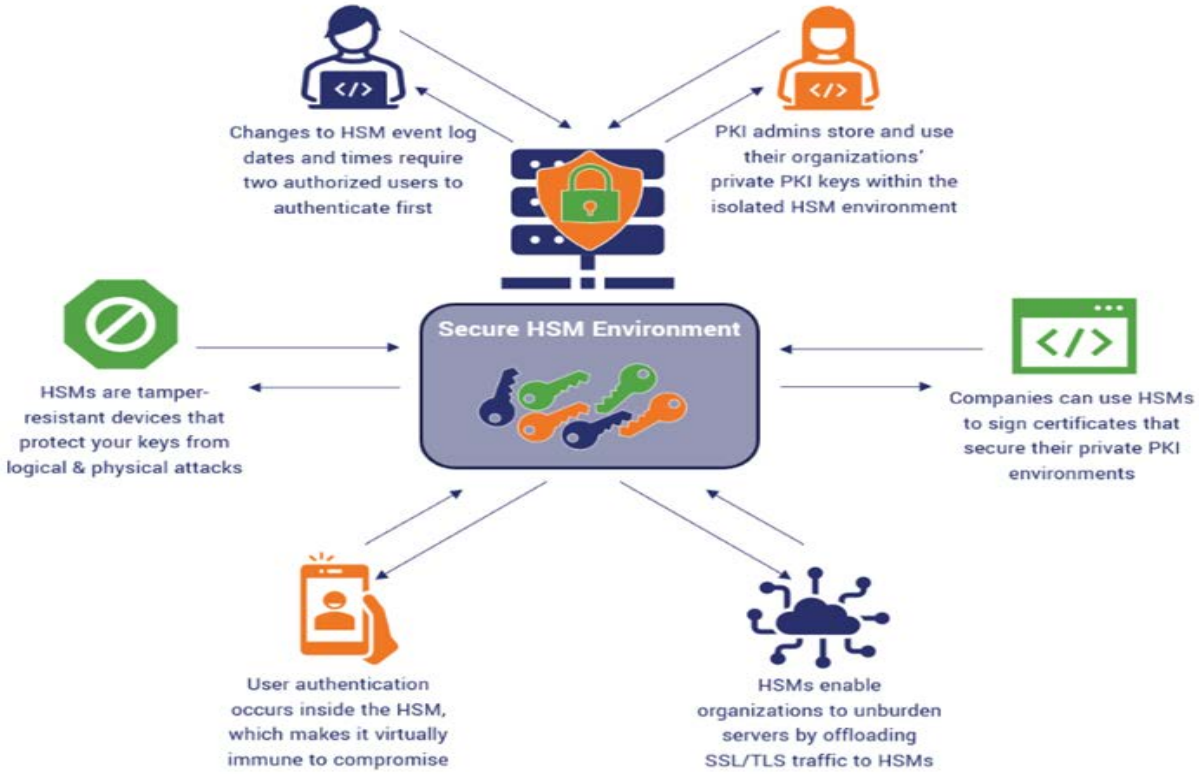
- Η ασφάλεια βάσει υλικού είναι μία από τις πιθανές λύσεις για τη βελτίωση των υφιστάμενων μηχανισμών ασφαλείας. Η ασφάλεια που βασίζεται σε υλικό χρησιμοποιεί ένα αποκλειστικό ολοκληρωμένο κύκλωμα υλικού ή επεξεργαστή για την εκτέλεση κρυπτογραφικών λειτουργιών και την αποθήκευση των κλειδιών. Μπορούν να αποτρέψουν την πρόσβαση ανάγνωσης και εγγραφής στα δεδομένα και να προσφέρουν ισχυρότερη προστασία από διάφορες επιθέσεις. Οι μηχανισμοί που βασίζονται σε υλικό, όπως το HSM, έχουν χρησιμοποιηθεί για επεξεργασία κρυπτογράφησης και ισχυρό έλεγχο ταυτότητας όπου μπορεί να κρυπτογραφήσει, να αποκρυπτογραφήσει, να αποθηκεύσει και να διαχειριστεί τα ψηφιακά κλειδιά. Τα HSM, μονάδες ασφαλείας υλικού που σχεδιάστηκαν για να προστατεύουν και να διαχειρίζονται ψηφιακά κλειδιά, έχουν χρησιμοποιηθεί μαζί με μηχανισμούς λογισμικού όπως PKI, AES για την κρυπτογράφηση των μηνυμάτων τους [38].

Ένα από τα κύρια προβλήματα με τις λύσεις ασφαλείας που βασίζονται σε υλικό είναι ότι είναι επιρρεπείς στις επιθέσεις Man-in-the-Middle. Σε αυτές τις επιθέσεις, όταν κλαπεί η μονάδα ασφαλείας υλικού, οι εισβολείς μπορούν να κλωνοποιήσουν τη συσκευή. Αυτό μπορεί να συγκριθεί με μια απλή φυσική κλειδαριά και κλειδί, όπου το κλειδί κλέβεται και κλωνοποιείται για να μιμηθεί το πραγματικό κλειδί. Οι φυσικά μη κλωνοποιήσιμες συναρτήσεις (PUF) μπορούν να δώσουν λύση σε αυτό το πρόβλημα. Οι φυσικά μη κλωνοποιήσιμες συναρτήσεις εισήχθησαν από τους Gassend et al. το 2002 [39] ως πρωτόγονο ασφαλείας βασισμένο σε υλικό. Το PUF χρησιμοποιεί τις εγγενείς παραλλαγές κατασκευής σε μια συσκευή για να δημιουργήσει ένα δακτυλικό αποτύπωμα του υλικού που προσφέρει το πολύτιμο πλεονέκτημα της μη κλωνοποίησης

4.1. Αναγνώριση

Ορισμένες πρακτικές αντιμετώπισης των ζητημάτων ασφάλειας αναγνώρισης με χρήση PUFs είναι:

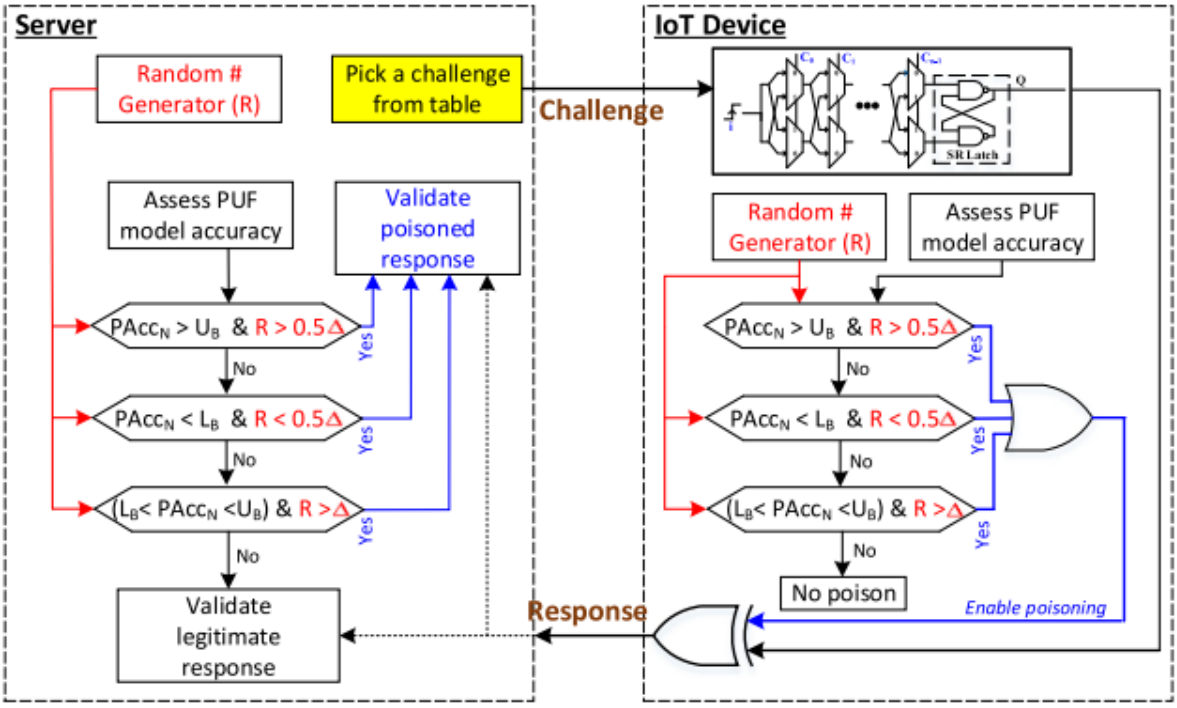
- Τα κλειδιά που παράγονται από την PUF πρέπει να αποθηκεύονται με ασφάλεια, όπως για παράδειγμα με χρήση μηχανισμών κρυπτογράφησης και χρήσης ασφαλούς αποθήκευσης.
- Η μονάδα PUF πρέπει να παραμένει απομονωμένη και να μην είναι προσβάσιμη από τρίτους. Αυτό μπορεί να επιτευχθεί με τη χρήση ασφαλούς αρχιτεκτονικής, όπως hardware security modules (HSMs) ή secure enclaves.



Σχήμα 15 Τρόποι με τους οποίους τα HSM βοηθούν στην ασφάλεια της ταυτότητας οντοτήτων IoT [51].

- Τα πρωτόκολλα επικοινωνίας βασισμένα σε PUF θα πρέπει να είναι ασφαλή. Αυτό περιλαμβάνει τη χρήση κρυπτογραφίας για την προστασία των δεδομένων και την εξασφάλιση της αυθεντικότητας και ακεραιότητας των μηνυμάτων.

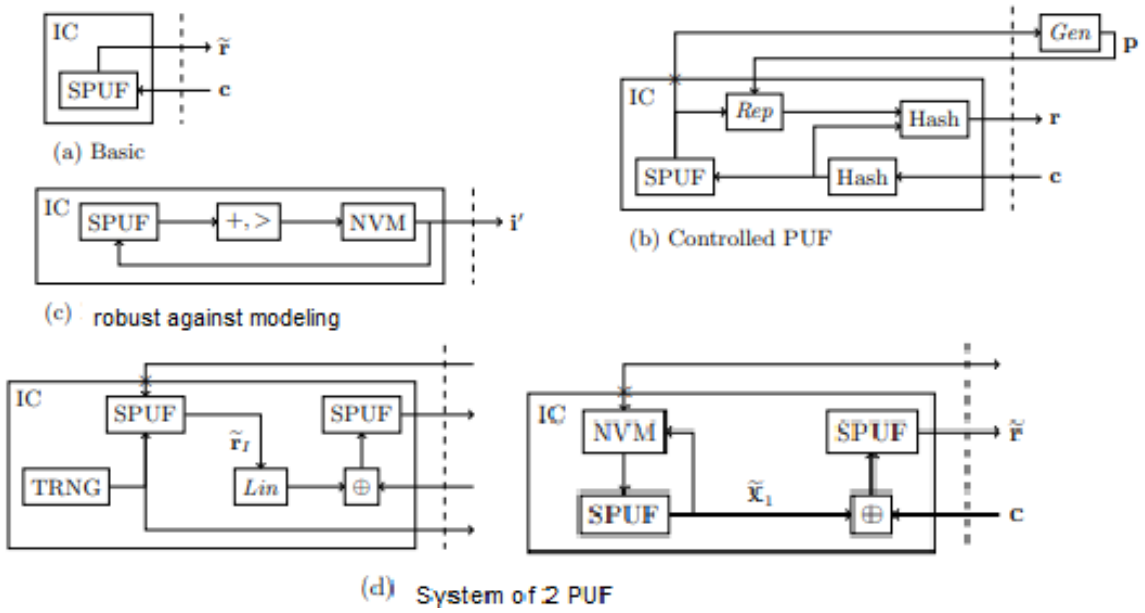
Δίνοντας έμφαση στον μετριασμό της ευπάθειας των σχημάτων ελέγχου ταυτότητας που βασίζονται σε PUF, ένας και ελαφρύς μηχανισμός περιορισμού του κινδύνου και ισχυρού ελέγχου ταυτότητας είναι οι μεθοδολογίες Adversarial Machine Learning (AML) [14]. Σύμφωνα με αυτές υποβαθμίζεται η ακρίβεια δεδομένων εισάγοντας λάθη. Μια τέτοια λανθασμένη εισαγωγή (δηλητηρίαση) αντιστοιχεί σε λάθος συσχέτιση πρόκλησης και απόκρισης, καθιστώντας την μη προβλέψιμη σε έναν επιτιθέμενο. Η ιδέα είναι να ξεγελάσουν τον ταξινομητή μοντελοποίησης PUF του εισβολέα εισάγοντας θόρυβο σε ορισμένα από τα στοιχεία δεδομένων έτσι ώστε να ταξινομούνται εσφαλμένα. Η απόδοση της μεθόδου εξαρτάται από το πλήθος των «δηλητηριασμένων» μηνυμάτων σε σχέση με τα αυθεντικά.



Σχήμα 16 Μπλοκ διαγράμματος της λειτουργίας «δηλητηρίασης» μηνυμάτων από την πλευρά του διακομιστή και της συσκευής IoT [14].

4.2. Έλεγχος ταυτότητας

Στο [27], οι προτείνει περισσότερη έρευνα σχετικά με τη θεμελιώδη φυσική ενός PUF προκειμένου να δημιουργηθεί ένα πραγματικά ισχυρό. Στο Σχήμα 7 παρουσιάζονται διαφορετικοί μηχανισμοί παραγωγής PUF οι οποίοι βελτιώνουν την αντοχή του μηχανισμού ελέγχου ταυτότητας σε επιθέσεις με ισχυρό PUF. Ορισμένα από τα πρωτόκολλα μπορεί να αξιοποιήσουν το ισχυρό PUF για να παρέχουν αντίσταση στην επίθεση πλευρικού καναλιού (side channel attack), αλλά η φυσική επίθεση (physical attack) μπορεί ακόμα να εξαπολυθεί εναντίον τους προσθέτοντας με τη χρήση ενός μπλοκ μηχανικής εκμάθησης.

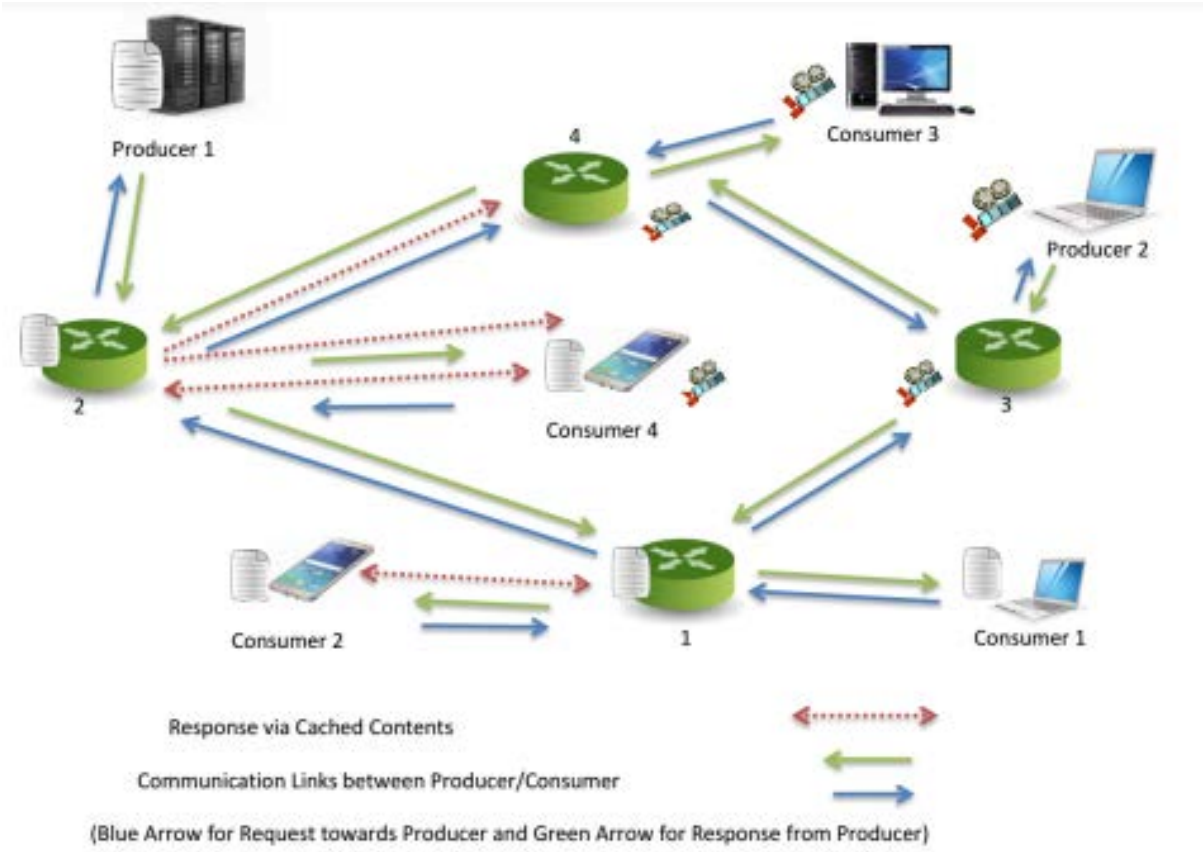


Σχήμα 17 Μηχανισμοί ενίσχυσης PUF έναντι επιθέσεων [27].

Στο [52] μελετάται η εφαρμογή της κβαντικής τεχνολογίας στην κρυπτογραφία και ειδικότερα τη φυσική ασφάλεια, και προτείνεται ένας νέος τύπος PUF που ονομάζονται μετακβαντικό PUF.

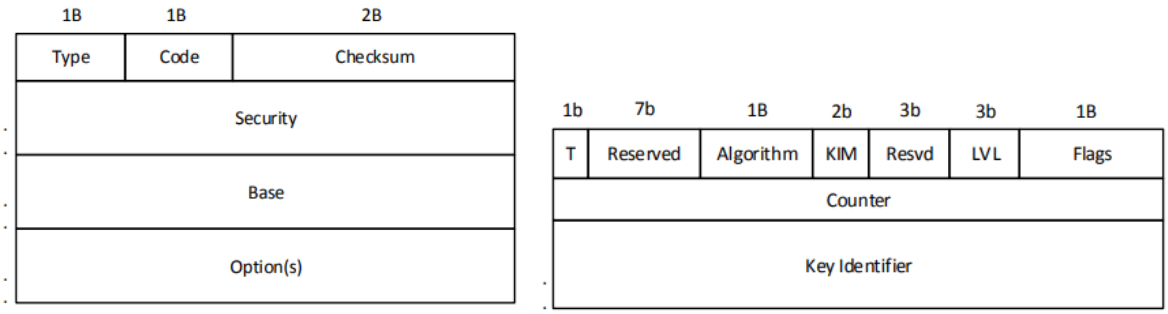
4.3. Κρυπτογράφηση

Στο [45], εισήχθη η χρήση της πληροφοριοκεντρικής δικτύωσης (ICN) ως πιθανό πρωτόκολλο για την αντιμετώπιση επιθέσεων σε συσκευές IoT όσον αφορά την προσωρινή αποθήκευση εντός του δικτύου, τα σχήματα ονοματοδοσίας, τα σχήματα ασφαλείας και τα σχήματα χειρισμού κινητικότητας. Οι συντάκτες του [44] τονίζουν την ανάγκη για «μεγαλύτερο και μόνιμο σχήμα ονοματοδοσίας και χώρο διευθύνσεων για περιεχόμενο και συσκευές IoT» [45].



Σχήμα 18 Λειτουργία ICN: Αιτήματα χρηστών για συγκεκριμένο περιεχόμενο από πλησιέστερους δρομολογητές (1,2,3,4), απαντήσεις εξυπηρετητών και ενδιάμεσοι κόμβοι. Υλοποιεί μηχανισμό ενδιάμεσης αποθήκευσης και περαιτέρω προώθησης του περιεχομένου αντί για δρομολόγηση από άκρο-σε-άκρο.

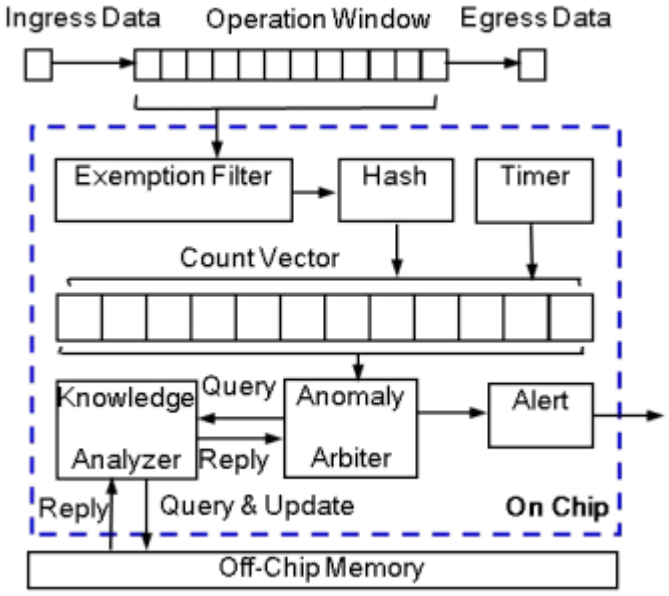
Στο [46], οι συγγραφείς εστίασαν στην ασφάλεια των επικοινωνιών μεταξύ συσκευών IoT χρησιμοποιώντας διαφορετικά πρωτόκολλα και μηχανισμούς.



Σχήμα 19 Μήνυμα ασφαλούς ελέγχου πρωτοκόλλου (Routing Protocol for Low-power and Lossy Networks (RPL)) και μέρος ασφαλείας του μηνύματος [46].

Στο [47], οι συγγραφείς συζήτησαν τη χρήση προγραμματιζόμενου υλικού όπως τα FPGA στην ασφάλεια της υποδομής δικτύου. Τονίστηκε ο ρόλος των μηχανισμών που βασίζονται σε υλικό για την αντιμετώπιση ορισμένων από τις προκλήσεις που παρουσιάζονται στις μεθόδους που βασίζονται σε

λογισμικό, καθώς και τις πιθανές προκλήσεις λόγω των αυξανόμενων απαιτήσεων για εντατική ανάλυση και λειτουργία σε πραγματικό χρόνο για διαδοχική επεξεργασία.



Σχήμα 20 Μπλοκ διάγραμμα για ανίχνευση ανωμαλίας ωφέλιμου φορτίου πληροφορίας [47].

4.4. Εμπιστευτικότητα

Ορισμένες πρακτικές αντιμετώπισης των ζητημάτων ασφαλείας εμπιστευτικότητας με χρήση PUFs, είναι:

- Κρυπτογραφία για την προστασία των δεδομένων που ανταλλάσσονται μεταξύ των συσκευών IoT και του κεντρικού διακομιστή. Αυτό εξασφαλίζει ότι μόνο οι εξουσιοδοτημένοι αποδέκτες μπορούν να αποκρυπτογραφήσουν τα δεδομένα.
- Περιορισμός της πρόσβασης στα δεδομένα με αυστηρά μέτρα ελέγχου πρόσβασης και αποκλεισμό πρόσβασης σε μη εξουσιοδοτημένους χρήστες.
- Προστασία της φυσικής ασφάλειας της συσκευής με αποτροπή φυσικής πρόσβασης από μη εξουσιοδοτημένα άτομα και την προστασία της συσκευής από κλοπή ή απώλεια.

4.5. Παρεμβολή

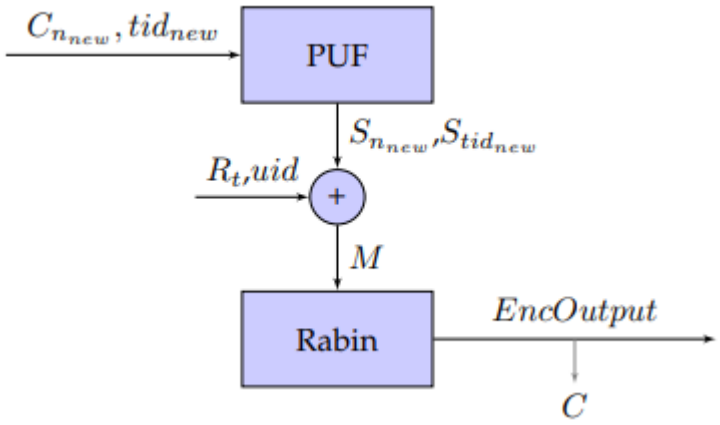
Αντιμετώπισης της παρεμβολής γίνεται με:

- Επαλήθευση της γνησιότητάς με αξιόπιστους μηχανισμούς για να εξασφαλιστεί ότι η PUF λειτουργεί σωστά και δεν έχει υποστεί παρεμβολή.

- Χρησιμοποίηση ασφαλών πρωτοκόλλων επικοινωνίας για την ανταλλαγή δεδομένων μεταξύ των συσκευών IoT και του κεντρικού διακομιστή.
- Επαλήθευση της αυθεντικότητας των μηνυμάτων που ανταλλάσσονται μεταξύ των συσκευών IoT. Μπορεί να γίνει μέσω ψηφιακών υπογραφών ή άλλων μηχανισμών που επαληθεύουν ότι τα μηνύματα προέρχονται από αξιόπιστες πηγές.

4.6. Κλωνοποίηση

Οι επιθέσεις κλωνοποίησης έχουν επίσης αποδειχθεί ότι είναι εφικτές, γεγονός που υπονομεύει σοβαρά τις δυνατότητες της τεχνολογίας για προστασία από την παραχάραξη. Μια λύση σε αυτό το πρόβλημα είναι ένα ελαφρύ πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας τριών μερών και ένα πρότυπο κατά της παραχάραξης. Η προτεινόμενη λύση είναι ο συνδυασμός του σχήματος κρυπτογράφησης δημόσιου κλειδιού Rabin με την τεχνολογία φυσικά μη κλωνοποιήσιμων συναρτήσεων (PUF) [15].



Σχήμα 21 Το σχήμα απόκρυψης απόκρισης χρησιμοποιώντας τον αλγόριθμο Rabin [15].

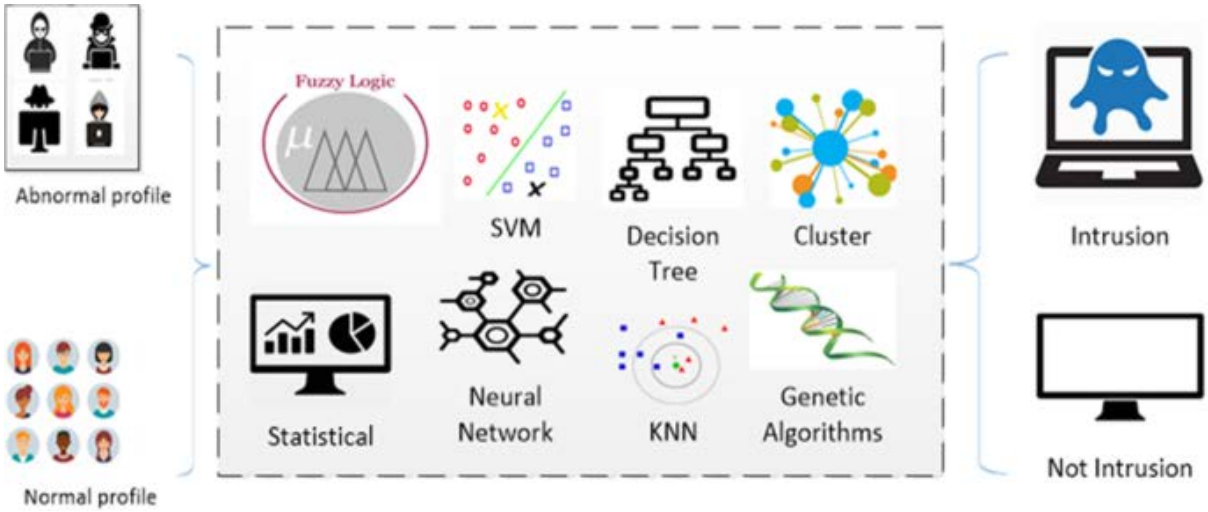
4.7. Διείσδυση

Οι πρακτικές αντιμετώπισης των ζητημάτων ασφάλειας διείσδυσης στο IoT είναι σημαντικές για τη διασφάλιση της ασφάλειας των συσκευών και των δικτύων. Παρακάτω παραθέτω ορισμένες πρακτικές αντιμετώπισης, με αναφορά σε μια πηγή για περαιτέρω ανάγνωση [13]:

- Εφαρμογή ισχυρών μέτρων αυθεντικοποίησης και εξουσιοδότησης: Αναγνωρίστε τις συσκευές IoT και εφαρμόστε ισχυρά μέτρα αυθεντικοποίησης και εξουσιοδότησης πριν επιτρέψετε την πρόσβασή τους στο δίκτυο. Αυτό περιλαμβάνει τη χρήση μοναδικών διαπιστευτηρίων και πιστοποιητικών.
- Ενίσχυση της ασφάλειας του δικτύου: Εφαρμόστε μέτρα ασφάλειας στο επίπεδο του δικτύου, όπως τον περιορισμό της πρόσβασης στις συσκευές, τη χρήση ενισχυμένων ρυθμίσεων ασφαλείας στους

δρομολογητές και τους φραγμούς προστασίας, καθώς και την απομόνωση του IoT δικτύου από άλλα ετερογενή δίκτυα.

- Αναβάθμιση των συσκευών και λογισμικού: Εξασφαλίστε ότι οι συσκευές IoT και το λογισμικό τους είναι ενημερωμένα με τις τελευταίες ενημερώσεις ασφαλείας και παρακολουθείστε τακτικά για τυχόν ευπάθειες ή αδυναμίες ασφάλειας.
- Χρήση κρυπτογραφίας: Εφαρμόστε μηχανισμούς κρυπτογράφησης για την προστασία των δεδομένων που ανταλλάσσονται ανάμεσα στις συσκευές IoT και τον κεντρικό διακομιστή.



Σχήμα 22 Μηχανισμοί IDS για συστήματα IoT [52]

4.8. Ιδιωτικότητα

Η ιδιωτικότητα είναι αποτέλεσμα όλων των προαναφερθέντων περιοχών προβλημάτων ασφαλείας, οπότε διαρρέεται οριζόντια από τα προηγούμενα. Αναλυτικότερα περιοχές που μπορούν να αντιμετωπίσουν πρακτικά ζητήματα ιδιωτικότητας είναι:

- Κάθε PUF χρησιμοποιείται αποκλειστικά από ένα συγκεκριμένο σύστημα IoT. Αυτό μειώνει τον κίνδυνο κλοπής ή αντιγραφής του PUF και μεγιστοποιεί την ιδιωτικότητα.
- Το περιβάλλον στο οποίο εκτελείται το σύστημα IoT με PUF είναι ασφαλές. Αυτό σημαίνει ότι πρέπει να ελέγχονται οι πρόσβαση στον υλικό και οι πιθανές επιθέσεις φυσικής πρόσβασης.
- Χρησιμοποιήστε τεχνικές απομόνωσης για την προστασία του PUF και των παραγόμενων κλειδιών. Απομονώστε το PUF από το υπόλοιπο σύστημα και χρησιμοποιήστε ασφαλείς κανάλια επικοινωνίας για τη μεταφορά των κλειδιών.
- Χρησιμοποιήστε κρυπτογραφία για την προστασία των δεδομένων που ανταλλάσσονται μεταξύ του συστήματος IoT και του PUF. Βεβαιωθείτε ότι τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται για την προστασία των δεδομένων είναι ασφαλή και παράγονται από το PUF.

- Βεβαιωθείτε ότι το λογισμικό του συστήματος IoT είναι ενημερωμένο και ασφαλές. Ενημερώνετε το λογισμικό για να διορθώνονται ενδεχόμενες ευπάθειες ασφαλείας και να προστατεύεται η ιδιωτικότητα των δεδομένων.
- Εφαρμόστε συστήματα παρακολούθησης και ανίχνευσης παραβιάσεων για τον εντοπισμό και την αντίδραση σε πιθανές απειλές στην ιδιωτικότητα. Αυτό μπορεί να περιλαμβάνει την ανίχνευση ανεπιθύμητων προσπαθειών πρόσβασης ή την παρακολούθηση των ακολουθιών χρήσης του συστήματος.

4.9. Παράθεση πρακτικών αντιμετώπισης θεμάτων ασφαλείας συσκευών IoT

Σύμφωνα με την ανάλυση που προηγήθηκε, τα θέματα ασφαλείας συστημάτων που περιλαμβάνουν IoT αναλύονται σε 8 θεματικές περιοχές. Για κάθε θεματική περιοχή εξετάστηκαν, βάσει της βιβλιογραφίας, διαφορετικές πρακτικές αντιμετώπισης τους. Η αντιστοίχιση αυτή αναλύεται ακολούθως στον Πίνακα 1.

Πίνακας 1 Αντιστοίχιση πρακτικών σε προβλήματα ασφαλείας συστημάτων IoT

ΠΡΟΒΛΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ	ΠΡΑΚΤΙΚΕΣ	ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Αναγνώριση - Παθητικές επιθέσεις - Ενεργητικές επιθέσεις - Προφίλ υψηλού επιπέδου - Προφίλ χαμηλού επιπέδου	hardware security modules (HSMs) secure key storage ασφαλή πρωτόκολλα επικοινωνίας	Παραμένει απομονωμένη και δεν είναι προσβάσιμη από τρίτους Τα κλειδιά αποθηκεύονται με ασφάλεια Αντοχή σε επιθέσεις υψηλού και χαμηλού προφίλ	Είναι στατικά και εξαρτώνται από την κατασκευή του υλικού Πιο ακριβή υλοποίηση
Έλεγχος ταυτότητας - Μοναδική ταυτότητα - Προστασία κλειδιών - Επίθεση εξαντλητικής αναζήτησης - Επίθεση μεσάζοντα	ισχυρό PUF μπλοκ μηχανικής εκμάθησης μετακβαντικό PUF	αντίσταση στην επίθεση πλευρικού καναλιού αντίσταση σε φυσική επίθεση φυσική ασφάλεια	Επιπλέον απαιτήσεις κατά την υλοποίηση Περισσότερη υπολογιστική ισχύ Περισσότερη έρευνα
Κρυπτογράφηση - Φυσικό επίπεδο - Επίπεδο δικτύου - Επίπεδο εφαρμογής - Επίπεδο διαχείρισης	μεγαλύτερο και μόνιμο σχήμα ονοματοδοσίας προγραμματιζόμενου υλικού όπως τα FPGA σχήματα χειρισμού κινητικότητας	Στατική ταυτοποίηση των συσκευών IoT Πολύ ισχυρά κλειδιά και πολύ γρήγορα Δημιουργία υπερσυνόλων έμπιστων συσκευών	Περιορισμός στη δυναμική μεταβολή των δικτύων Εξειδικευμένος ακριβός εξοπλισμός Περιορισμός στη δυναμική μεταβολή των δικτύων

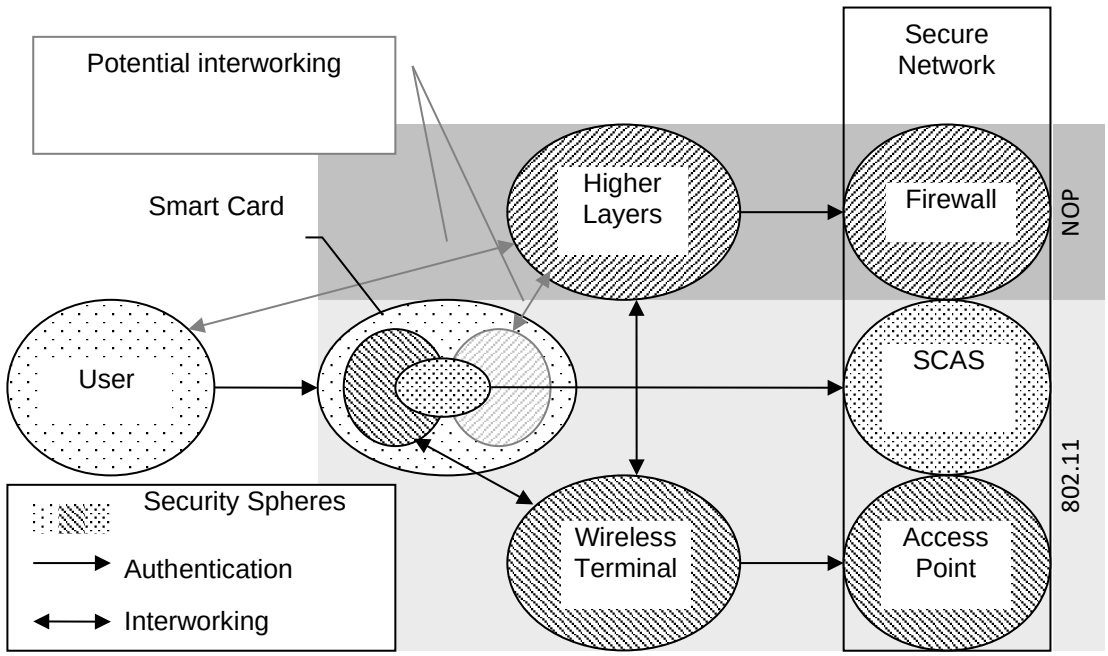
Εμπιστευτικότητα	Περιορισμός πρόσβασης Κρυπτογραφία	Έλεγχος της πρόσβασης από τρίτους Αποκλεισμός στην πρόσβαση στο περιεχόμενο από τρίτους	
Παρεμβολή - Φυσικό επίπεδο - Επίπεδο λογικής σύνδεσης - Επίπεδο δικτύου - Επίπεδο μεταφοράς - Επίπεδο εφαρμογής	Επαλήθευση της γνησιότητάς Ψηφιακές υπογραφές Χρησιμοποίηση ασφαλών πρωτοκόλλων επικοινωνίας	Εξασφαλίζεται ότι λειτουργεί σωστά και δεν έχει υποστεί παρεμβολή Επαλήθευση της αυθεντικότητας των μηνυμάτων	Καθυστέρηση στην επικοινωνία Πολύπλοκές διαδικασίες επικοινωνίας
Κλωνοποίηση - Φυσικό επίπεδο - Επίπεδο δικτύου	δημόσιο κλειδί Rabin σε συνδυασμό με PUF	Πρωτόκολλο αμοιβαίου ελέγχου ταυτότητας τριών μερών και πρότυπο κατά της παραχάραξης	
Διείσδυση - Κατασκευαστικές αδυναμίες - Αδύναμα πρωτόκολλα - Μη ασφαλείς συνδέσεις - Ελλιπής διαχείριση και ενημέρωση	Ενημερώσεις Ισχυρά μέτρα ασφάλειας και περιφρούρησης δικτύου	Αναβάθμιση λογισμικού και περιορισμός ευπαθειών Αποτροπή διεισδύσεων και παρεισφρήσεων.	Πολύπλοκο σύστημα συσκευής IoT Κόστος διαχείρισης και λειτουργίας
Ιδιωτικότητα	Συνδυασμός των παραπάνω	Συνδυασμός των παραπάνω	Συνδυασμός των παραπάνω

Από τα παραπάνω συμπεραίνουμε ότι δεν υπάρχει μία μοναδική πρακτική που να αντιμετωπίζει αποτελεσματικά τα προβλήματα συστημάτων που περιλαμβάνουν IoT αλλά ένας συνδυασμός τους. Σε πολλές περιπτώσεις η αποτελεσματική αναγνώριση της ταυτότητας των μερών αλλά και η κρυπτογράφηση της μεταξύ τους επικοινωνίας είναι κομβικής σημασίας. Στην κατεύθυνση αυτή η τεχνική των PUF συμβάλει θετικά, αν και όχι ολοκληρωτικά, στην επίλυση των προβλημάτων ασφαλείας. Η πρακτική είναι πολλά υποσχόμενη και μπορεί να αξιοποιήσει τις σύγχρονες τεχνολογικές εξελίξεις, δηλαδή την κβαντική υπολογιστική και την τεχνητή νοημοσύνη.

5ο ΚΕΦΑΛΑΙΟ: ΣΥΜΠΕΡΑΣΜΑΤΑ

Με την εργασία αυτή εμβαθύναμε στα προβλήματα ασφαλείας συστημάτων και συσκευών IoT καθώς και στα χαρακτηριστικά τους. Αναλύοντας τις επιμέρους επιδράσεις ευπαθειών και απειλών ασφαλείας αναδείξαμε μέσα από την βιβλιογραφία τις βασικότερες πρακτικές αντιμετώπισης των θεμάτων αυτών. Τα προβλήματα ασφαλείας αναλύθηκαν σε οκτώ (8) θεματικές περιοχές προκειμένου να διατρέξουμε αναλυτικά τα χαρακτηριστικά τους. Οι πρακτικές αντιμετώπισης των θεμάτων ασφαλείας δεν είναι το ίδιο αποτελεσματικές για τα προβλήματα κάθε θεματικής περιοχής αλλά είναι περισσότερο εξειδικευμένες. Μια προσεκτική αντιπαράθεση των πρακτικών έναντι των προβλημάτων μπορεί να αναδείξει βέλτιστες πρακτικές με ή χωρίς τον συνδυασμό τους.

Από τις τεχνολογίες που χρησιμοποιούνται στην αντιμετώπιση προβλημάτων ασφαλείας σε περιορισμένα περιβάλλοντα όπως είναι αυτά των συσκευών IoT ξεχωρίζει η PUF. Συνδυάζει αποτελεσματικά τα κατασκευαστικά χαρακτηριστικά της εκάστοτε συσκευής για την υποστήριξη των λειτουργιών ασφαλείας και ταυτόχρονα λειτουργεί αποδοτικά στο περιβάλλον εφαρμογής. Μπορεί να χρησιμοποιηθεί σε περισσότερες από μία θεματικές περιοχές ασφαλείας όταν το πρόβλημα βασίζεται στην ταυτοποίηση και την κρυπτογράφηση. Ενδιαφέρουσα θα ήταν η ενοποίηση της τεχνολογία PUF σε ασφαλή περιβάλλοντα όπως αυτό της έξυπνης κάρτας [49] και η εξέλιξη τους προς ένα ταχύτερο επεξεργαστικά περιβάλλον. Μια άλλη ενδιαφέρουσα κατεύθυνση θα ήταν η εμπλοκή της τεχνολογίας BlockChain στην διαδικασία επικοινωνίας αποκεντρωμένων συσκευών σε περιβάλλοντα IoT, προοπτική η οποία βρίσκει προσχώματα στις υψηλές απαιτήσεις επεξεργαστικής ισχύος.



Σχήμα 23 Σύστημα ασφαλείας βασισμένο σε Hidden layer Authentication [49].

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Alrawais, A., Alhothaily, A., Hu, C., Cheng, X., & Wan, J. (2017). Internet of Things security: A survey. Journal of Ambient Intelligence and Humanized Computing, 8(5), 639-665.

[2] Wang, H., Jin, Z., Yuan, X., & Cao, J. (2018). A Survey on Intrusion Prevention Systems for Internet of Things. IEEE Access, 6, 37220-37233.

[3] Nikolaidis, E., Loukas, G., Gouglidis, A., & Panaousis, E. (2017). Ensuring Security and Privacy in Smart Cities with Blockchain Technology. IEEE Access, 5, 2059-2068.

[4] Gai, K., Guizani, M., Yang, Y., & Zhou, W. (2017). RSA-Based Security Protocol for IoT Applications. IEEE Internet of Things Journal, 4(6), 2068-2077.

[5] Amsalem, Y., & Herzberg, A. (2017). Securing the Internet of Things—A Standardization Perspective. IEEE Internet of Things Journal, 4(6), 2133-2144.

[6] Raza, S., Wallgren, L., & Voigt, T. (2018). A survey on self-healing mechanisms for Internet of Things. IEEE Communications Surveys & Tutorials, 20(3), 2408-2427.

[7] F. Siddiqui, M. Hagan and S. Sezer. (2018). Embedded policing and policy enforcement approach for future secure IoT technologies. Living in the Internet of Things: Cybersecurity of the IoT, London. pp. 1-10, doi: 10.1049/cp.2018.0010.

[8] C. Sun, R. Xing, Y. Wu, G. Zhou, F. Zheng and D. Hu. (2021). Design of Over-the-Air Firmware Update and Management for IoT Device with Cloud-based RESTful Web Services. China Automation Congress (CAC), Beijing, China. pp. 5081-5085, doi: 10.1109/CAC53003.2021.9727516.

[9] Y. Brun, J. y. Bang, G. Edwards and N. Medvidovic. (2015), Self-Adapting Reliability in Distributed Software Systems. IEEE Transactions on Software Engineering, vol. 41, no. 8, pp. 764-780, 1 Aug. doi: 10.1109/TSE.2015.2412134.

[10] Michael Karner, Philipp Moll, Thomas Menzel, και Christoph Meinel. (2018). A Review of Software Update Methods for IoT Devices. IEEE Internet of Things Journal, volume 5, number 2, pp 826-838, April.

[11] H. Kim and E. A. Lee. (2017). Authentication and Authorization for the Internet of Things. IT Professional, vol. 19, no. 5, pp. 27-33. doi: 10.1109/MITP.2017.3680960.

[12] Samie F., Tsoutsouras V., Bauer L., Xydis S., Soudris D., Henkel J. (2016) Computation offloading and resource allocation for low-power IoT edge devices Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on, IEEE , pp. 7-12

[13] Top 10 IoT vulnerabilities and how to avoid them. ENISA: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot-security-challenges/iot-top-10-risks

[14] Wassila Lalouani, Mohamed Younis, Mohammad Ebrahimabadi, and Naghmeh Karimi. (2022). Countering Modeling Attacks in PUF-based IoT Security Solutions. J. Emerg. Technol. Comput. Syst. 18, 3, Article 46 (July 2022), 28 pages. https://doi.org/10.1145/3491221

[15] Yildiran Yilmaz, Viet-Hoa Do and Basel Halak. (?). ARMOR: An anti-counteRfeit security Mechanism for lOw cost Radio frequency identification systems. School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK. (https://eprints.soton.ac.uk/437405/1/rabin_paper_EToC_revised.pdf)

[16] O. El Mouaatamid, M. Lahmer, M. Belkasmi. (2016). Internet of things security: Layered classification of attacks and possible countermeasures, Electron. J. Inform. Technol. 9

[17] A. Botta, W. De Donato, V. Persico, A. Pescapı. (2014). On the integration of cloud computing and internet of things. International Conference on Future Internet of Things and Cloud, IEEE, 2014, pp. 23–30.

[18] I.A.T. Hashem, V. Chang, N.B. Anuar, K. Adewole, I. Yaqoob, A. Gani, E. Ahmed, H. Chiroma. (2016). The role of big data in smart city, Int. J. Inf. Manage. 36 (5) 748–758.

[19] M.M. Hossain, M. Fotouhi, R. Hasan. (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things, in: Services (SERVICES), 2015 IEEE World Congress on, IEEE, pp. 21–28.

[20] S. Alam, D. De. (2014). Analysis of security threats in wireless sensor networks. arXiv preprint arXiv:1406.0298.

[21] A. Mayzaud, R. Badonnel, I. Chrisment. (2016). A taxonomy of attacks in RPL-based internet of things, Int. J. Netw. Secur. 18 (3) 459–473.

[22] U. Sabeel, S. Maqbool. (2013). Categorized security threats in the wireless sensor networks: Countermeasures and security management schemes, Int. J. Comput. Appl. 64 (16.

[23] A.W. Atamli, A. Martin. (2014). Threat-based security analysis for the Internet of Things, in: 2014 International Workshop on Secure Internet of Things, IEEE, pp. 35–43.

[24] Y. Lu, L. Da Xu. (2018). Internet of Things (IoT) cybersecurity research: a review of current research topics, IEEE Internet Things J. 6 (2) 2103–2115.

[25] H. Lin, N. Bergmann. (2016). IoT privacy and security challenges for Smart Home Environments, Information 7 (3) 44.

[26] E. Baccelli, C. Góndoğan, O. Hahm, P. Kietzmann, M.S. Lenders, H. Petersen, K. Schleiser, T.C. Schmidt, M. Wδhlisch. (2018). RIOT: An open source operating system for low-end embedded devices in the IoT, IEEE Internet Things J. 5 (6) 4428–4440.

[27] J. Delvaux, R. Peeters, D. Gu, I. Verbauwhede. (2015). A survey on lightweight entity authentication with strong PUFs, ACM Comput. Surv. 48 (2) 1–42.

[28] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) 1125–1142

[29] A. Mosenia, N.K. Jha. (2017). A comprehensive study of security of internet-of-things, IEEE Trans. Emerg. Top. Comput. 5 (4) 586–602.

[30] S.K. Sanadhya, P. Sarkar. (2008). New collision attacks against up to 24-step SHA-2, in: International Conference on Cryptology in India, Springer, pp. 91–103.

[31] L.M.R. Tarouco, L.M. Bertholdo, L.Z. Granville, L.M.R. Arbiza, F. Carbone, M. Marotta, J.J.C. de Santanna. (2012). Internet of things in healthcare: Interoperatibility and security issues, Communications (ICC), IEEE International Conference on, IEEE, 2012, pp. 6121–6125.

[32] P. Varga, S. Plosz, G. Soos, C. Hegedus. (2017). Security threats and issues in automation IoT Factory Communication Systems (WFCS), IEEE 13th International Workshop on, IEEE, 2017, pp. 1–6.

[33] C. Karlof, D. Wagner. (2003). Secure Routing in Sensor Networks: Attacks and Countermeasures.

[34] I. Krontiris, T. Giannetsos, T. Dimitriou. (2008). Launching a Sinkhole attack in wireless sensor Networks; the intruder side, in: IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, IEEE, pp. 526–531.

[35] D. Senie, P. Ferguson. (1998). Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing, Network.

[36] K. Sharma, M. Ghose. (2010). Wireless sensor networks: An overview on its security threats, IJCA 42–45, Special Issue on ‘‘Mobile Ad-hoc Networks’’ MANETs.

[37] K.S. Win. (2008). Analysis of detecting Wormhole Attack in wireless networks, in: World Academy of Science, Engineering and Technology, Citeseer, pp. 422–428.

[38] W. Eddy. (2007). TCP SYN Flooding Attacks and Common Mitigations, Tech. rep., RFC.

[39] L. Joncheray. (1995). A simple active attack against TCP, in: USENIX Security Symposium, pp. 2–15.

[40] M. Manzo, T. Roosta, S. Sastry. (2005). Time synchronization attacks in sensor networks, in: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, ACM, pp. 107–116.

[41] A. Becher, Z. Benenson, M. Dornseif. (2006). Tampering with motes: Real-world physical attacks on wireless sensor networks, in: International Conference on Security in Pervasive Computing, Springer, pp. 104–118.

[42] J. Liu, Y. Xiao, C.P. Chen. (2012). Authentication and access control in the internet of things, in: Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference on, IEEE, pp. 588–592.

[43] K. Zhang, X. Liang, R. Lu, X. Shen. (2014). Sybil attacks and their defenses in the internet of things, IEEE Internet Things J. 1 (5) 372–383.

[44] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet Things J. 4 (5) 1125–1142.

[45] S. Arshad, M.A. Azam, M.H. Rehmani, J. Loo. (2018).Recent advances in informationcentric networking based internet of things (ICN-IoT), IEEE Internet Things J.

[46] J. Granjal, E. Monteiro, J.S. Silva. (2015). Security for the internet of things: a survey of existing protocols and open research issues, IEEE Commun. Surv. Tutor. 17 (3) 1294–1312.

[47] H. Chen, Y. Chen, D.H. Summerville. (2011). A survey on the application of FPGAs for network infrastructure security, IEEE Commun. Surv. Tutor. 13 (4) 541–561.

[48] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone. (2016). Report on Post-Quantum Cryptography, US Department of Commerce, National Institute of Standards and Technology.

[49] Pikrammenos, G., Sarkis, G., Soldatos, J., Anagnostopoulos, V. (2003). Hidden Layer Authentication Using Smart Card for WEP Based WLANs. In: Gritzalis, D., De Capitani di Vimercati, S., Samarati, P., Katsikas, S. (eds) Security and Privacy in the Age of Uncertainty.

SEC 2003. IFIP — The International Federation for Information Processing, vol 122. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35691-4_44

[50] A. Shamsoshoara, A. Korenda, F. Afghah, S. Zeadally. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Elsevier, Computer Networks 183

[51] https://www.thesslstore.com/blog/what-is-a-hardware-security-module-hsms-explained/, accessed on 13/7/2023

[52] A. Abbasi, J. Wetzels, W. Bokslag, E. Zambon, S. Etalle. (2014). On emulation-based network intrusion detection systems. Research in attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17–19, 2014, pp. 384–404