ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΥΛΙΚΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

‘‘Ασφάλεια στο Διαδίκτυο των Πραγμάτων μέσω Φυσικών Μη Κλωνοποιήσιμων Συναρτήσεων’’

ΠΑΣΣΙΟΣ ΘΕΟΔΩΡΟΣ

71347421

Επιβλέποντες καθηγητές: Δρ. Εμμανουήλ Μιχαηλίδης
Δρ. Ιωάννης Βογιατζής , Καθηγητής

Διπλωματική εργασία υποβληθείσα στο Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών

του Πανεπιστημίου Δυτικής Αττικής

ΑΘΗΝΑ, ΙΟΥΛΙΟΣ 2021

Ασφάλεια στο Διαδίκτυο των Πραγμάτων μέσω Φυσικών Μη Κλωνοποιήσιμων Συναρτήσεων

ΠΑΣΣΙΟΣ ΘΕΟΔΩΡΟΣ

71347421

Επιβλέποντες καθηγητές: Δρ. Εμμανουήλ Μιχαηλίδης
Δρ. Ιωάννης Βογιατζής , Καθηγητής

Εγκρίθηκε από τη τριμελή εξεταστική επιτροπή

Ioannis Voyiatzis Digitally signed by Ioannis Voyiatzis Date: 2021.07.30 12:19:40 +03'00'	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2021.07.30 10:46:57 +03'00'	Emmanouil Michailidis Digitally signed by Emmanouil Michailidis Date: 2021.07.30 10:21:16 +03'00'
.....	.....	.....
Καθηγητής	Καθηγητής	Δρ. Εμμανουήλ Μιχαηλίδης
Ιωάννης Βογιατζής	Παναγιώτης Γιαννακόπουλος	

Πανεπιστήμιο Δυτικής Αττικής, Μηχανικών Πληροφορικής και Υπολογιστών
Πάσσιος Θεόδωρος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΥΛΙΚΟΥ

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ/ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Πάσσιος Θεόδωρος του Χρήστου, με αριθμό μητρώου 71347421 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι 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».

Ο Δηλών

Η έγκριση της διπλωματικής εργασίας δεν υποδηλοί την αποδοχή των γνωμών του συγγραφέα. Κατά τη συγγραφή τηρήθηκαν οι αρχές της ακαδημαϊκής δεοντολογίας.

ΠΕΡΙΛΗΨΗ

Το Διαδίκτυο των Πραγμάτων (Internet of Things – IoT) αποτελεί ένα από τα μεγαλύτερα τεχνολογικά επιτεύγματα και καθημερινά κερδίζει όλο και περισσότερο έδαφος στην καθημερινότητα των ανθρώπων. Στα πλαίσια του IoT διάφορες τεχνολογίες προσδίδουν την χαρακτηριστική λειτουργικότητα του. Διαφορετικές συσκευές που τις περισσότερες φορές βρίσκονται τοπολογικά απομακρυσμένα διασυνδέονται και ανταλλάσσουν δεδομένα και πληροφορίες. Παρά την συνεισφορά του σε πολλούς τομείς, προκλήσεις και ζητήματα ασφαλείας περιορίζουν την ευρεία υιοθέτησή του. Επιτιθέμενοι χρήστες εκμεταλλεύονται ευπάθειες του δικτύου, λογισμικού και υλικού, παραβιάζοντας βασικές δικλείδες ασφαλείας με σκοπό να προκαλέσουν διαρροή δεδομένων. Συμβατικοί μηχανισμοί ασφαλείας, οι οποίοι προστατεύουν παραδοσιακά τα ψηφιακά συστήματα, δεν ενδείκνυται για τα συστήματα IoT, καθώς οι συσκευές των συστημάτων IoT έχουν ιδιαίτερα χαρακτηριστικά, όπως η περιορισμένη ισχύ, η περιορισμένη μνήμη, η περιορισμένη υπολογιστική ικανότητα, η χαμηλή κατανάλωση ενέργειας, το κόστος αγοράς και το μέγεθος τους. Η έλλειψη ασφαλών μηχανισμών ασφαλείας, όπως η κρυπτογράφηση, δίνει περισσότερες ευκαιρίες σε κακόβουλους χρήστες να ξεκινούν επιθέσεις στις συσκευές του IoT. Για την αντιμετώπιση των κινδύνων είναι απαραίτητη η υιοθέτηση καινοτόμων μηχανισμών ασφαλείας. Σε αυτή την κατεύθυνση, οι φυσικές μη κλωνοποιήσιμες συναρτήσεις (Physically Unclonable Functions - PUFs) αποτελούν μία πολλά υποσχόμενη λύση. Ωστόσο, οι συμβατικές PUF παρουσιάζουν ευαισθησία σε κάποιες επιθέσεις, ενώ οι συσκευές IoT έχουν ιδιαίτερα χαρακτηριστικά. Συνεπώς, είναι απαραίτητη η χρήση ειδικά σχεδιασμένων PUF, οι οποίες εναρμονίζονται με τα ιδιαίτερα χαρακτηριστικά των IoT συσκευών και, επιπρόσθετα, παρουσιάζουν μεγαλύτερη ανθεκτικότητα απέναντι σε επιθέσεις.

Στην παρούσα διπλωματική εργασία, αρχικά γίνεται εισαγωγή σε γενικές έννοιες πάνω στο IoT, συμπεριλαμβανομένων τεχνολογιών αρχιτεκτονικής και βασικών χαρακτηριστικών του. Κατά δεύτερον, επιχειρείται σύντομη παρουσίαση των κινδύνων, καθώς και των επιθέσεων απέναντι στο IoT. Στο επόμενο στάδιο, παρατίθεται η τεχνολογία PUF ως πιθανή λύση ασφαλείας και αναφέρονται οι προκλήσεις της τεχνολογίας αυτής. Τέλος, παρουσιάζονται

ορισμένα είδη ειδικά σχεδιασμένων PUF, οι οποίες χαρακτηρίζονται από μεγαλύτερη ανθεκτικότητα και η χρήση τους ενδείκνυται για το IoT.

Λέξεις κλειδιά

Διαδίκτυο των Πραγμάτων, Φυσικές Μη Κλωνοποιήσιμες Συναρτήσεις, Ασφάλεια Υλικού.

Physical Unclonable Functions for Internet of Things Security

Passios Theodoros

The Internet of Things (IoT) is one of the greatest technological advances which is gaining more and more ground in people's daily lives. Within the framework of IoT, various technologies give its characteristic functionality. Different devices, are often located topologically remotely, interconnect and exchange data and information. Despite its contribution in many areas, challenges and security issues limit the adoption of IoT. Exploit network, software and hardware vulnerabilities by violating key security issues in order to cause data leakage. Conventional security devices, which protect traditional digital systems, are not suitable for IoT systems, as IoT devices are characterized by special features that prevent their use. Typical paradigms of such features include the limited power, limited memory, limited computing power, low power consumption, monetary cost and size. The lack of security mechanisms, such as encryption, on many of the Internet of Things' digital devices give more opportunities to potential attackers to attack these systems. To address the risks in IoT systems, it is necessary to adopt security mechanisms. The Physical Unclonable Functions (PUFs) constitute a promising lightweight security solution that utilizes the hardware characteristics of integrated circuits (ICs). However, specially designed PUFs are required within IoT that are compatible with the special features of IoT devices and are more resistant to attacks that tend to damage data privacy.

In this dissertation, we first introduce general concepts on IoT including key architectural technologies and key features. Secondly, a brief presentation of the dangers and the is provided. Next, the PUF technology is presented as a possible security solution and the challenges of this technology are underlined. Finally, some types of specially designed PUF for IoT are presented.

Keywords

Internet of Things, Physically Unclonable Functions, Hardware Security.

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΚΑΤΑΛΟΓΟΣ ΓΡΑΦΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΣΥΜΒΟΛΙΣΜΟΙ

IoT: Διαδίκτυο των Πραγμάτων

ML: Μηχανική Μάθηση

RE: Αντίστροφη Μηχανική

RO: Ταλαντωτής Δακτυλίου

PUF: Φυσική Μη-Κλωνοποιήσιμη Συνάρτηση

RFID: Radio Frequency Identification

DoS: Επιθέσεις Άρνησης Εξυπηρέτησης

DDoS: Επιθέσεις Κατανεμημένης Άρνησης Εξυπηρέτησης

PPUF: Δημόσια Φυσική Μη-Κλωνοποιήσιμη Συνάρτηση

C-PUF: Ελεγχόμενη Φυσική Μη-Κλωνοποιήσιμη Συνάρτηση

IC: Ολοκληρωμένο Κύκλωμα

CPR: Ζεύγος Πρόκλησης Απόκρισης

IP: Πνευματική Ιδιοκτησία

TCP: Πρωτόκολλο Ελέγχου Μεταφοράς

Re-RAM: Resistive Random Access Memory

2G: Δεύτερη Γενιά

3G: Τρίτη Γενιά

4G: Τέταρτη Γενιά

RF: Ραδιοσυχνότητα

BLE: Bluetooth χαμηλής ενέργειας

6LoWPAN: IPv6 Low-power Wireless Personal Area Networks

LHPUF: Ελαφριά υβριδική Φυσική Μη-Κλωνοποιήσιμη Συνάρτηση

FSM: Μηχανή πεπερασμένης κατάστασης

Wi-Fi: Wireless Fidelity

WSN: ασύρματο δίκτυο αισθητήρων

BLE: Bluetooth χαμηλής ενέργειας

IEEE: Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών

CPU: Κεντρική Μονάδα Επεξεργασίας

WLAN: Ασύρματο Τοπικό Δίκτυο

SaaS: Λογισμικό ως Υπηρεσία

PaaS: Πλατφόρμα ως Υπηρεσία

NaaS: Δίκτυα ως Υπηρεσία

IaaS: Υποδομή ως Υπηρεσία

GDPR: Γενικός Κανονισμός Προστασίας Δεδομένων

AES: Advanced Encryption Standard

DPA: Differential Power Analysis

SPA: Simple Power Analysis

Mem APUFs: PUFs βασισμένα στην μνήμη

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ

Στα πλαίσια της διπλωματικής μου εργασίας, θα επιθυμούσα να εκφέρω τις βαθύτατες ευχαριστίες μου στους επιβλέποντες καθηγητές μου, τον κ. Μιχαηλίδη Εμμανουήλ και τον κ. Βογιατζή Ιωάννη, οι οποίοι μου έδωσαν την ευκαιρία να ασχοληθώ με μία ενδιαφέρουσα θεματική ενότητα, και με βοήθησαν κατευθύνοντάς με στο να διαμορφώσω τη γνώμη μου πάνω στα σύγχρονα ζητήματα ασφαλείας του Διαδικτύου των Πραγμάτων καθώς και στην προστασία συσκευών μέσω Φυσικών Μη-Κλωνοποιήσιμων Συναρτήσεων. Η αμέριστη βοήθεια τους και η διαρκής επικοινωνία αποτέλεσε αρωγό για την εκπόνηση της διπλωματικής μου εργασίας στα πλαίσια της ολοκλήρωσης των σπουδών μου. Επιπρόσθετα, θα ήθελα να ευχαριστήσω τους ανθρώπους στον οικογενειακό μου κύκλο και τους κοντινούς μου ανθρώπους για την συνεχή στήριξη και για την πίστη τους στις ικανότητες και δυνατότητες μου.

ΚΕΦΑΛΑΙΟ 1 : ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Το IoT αποτελεί την κορύφωση της τεχνολογικής εξέλιξης. Με άλλα λόγια, πραγματοποιεί την εισαγωγή σε έναν κόσμο, όπου τα φυσικά αντικείμενα ενσωματώνονται απρόσκοπτα στο δίκτυο πληροφοριών και μπορούν να γίνουν ενεργά πλέον, συμμετέχοντας στις επιχειρηματικές διαδικασίες. Τα «πράγματα» αντιπροσωπεύουν τις ταυτότητες σύνδεσης στο διαδίκτυο εικονικών αντικειμένων [47]. (Floerkemeier, et al., 2008)

Εικόνα 1: Η έννοια του Διαδικτύου των Πραγμάτων[1].

1.1 ΕΙΣΑΓΩΓΗ

Η τεχνολογική εξέλιξη του διαδικτύου ώθησε την αύξηση της προσβασιμότητας σε αυτό. Όλο και περισσότεροι χρήστες από όλο τον κόσμο μπορούν άμεσα και

[1]https://web.archive.org/web/20180202162428/http://www.itech4u.gr/tech/hands-on/item/7262-internet-of-things-se-apla-ellinika

γρήγορα να συνδεθούν στο διαδίκτυο. Συνεπώς, ήταν φυσικό επακόλουθο η εκθετικά αυξανόμενη σύνδεση ψηφιακών συσκευών στο διαδίκτυο. Η φιλοσοφία του ελέγχου άλλων συσκευών και της απομακρυσμένης σύνδεσης συσκευών ήταν εξειδικευμένη για το λόγο του ότι χρειαζόταν ειδικός εξοπλισμός και ασύρματες συνδέσεις περιορισμένης εμβέλειας. Η δυνατότητα επικοινωνίας μίας συσκευής με άλλες απομακρυσμένες συσκευές έδωσε το έναυσμα να συνδέονται μεταξύ τους όλο και περισσότερες συσκευές μέσω διαδικτύου. Αυτό, αποτελεί την βασική ιδέα του διαδικτύου των πραγμάτων, η σύνδεση δηλαδή οποιασδήποτε συσκευής με το διαδίκτυο και η δυνατότητα απομακρυσμένου ελέγχου της συσκευής αυτής. Η έννοια του IoT σχετίζεται άμεσα όχι μόνο με συσκευές, οι οποίες χαρακτηρίζονται από την σύνδεση τους στο internet αλλά και με συσκευές που ανταλλάσσουν πληροφορίες με μεγάλα κεντρικά μηχανήματα τα οποία «αποφασίζουν», αναλαμβάνουν δράση και επεξεργάζονται χωρίς ανθρώπινη παρέμβαση, σύμφωνα με τον ορισμό που αποδόθηκε από τους οραματιστές και αναλυτές της τεχνολογίας. (i-TECH4u.gr, 2018-02-02)[6].

Ένας ακόμη ορισμός που μπορεί να δοθεί στην έννοια του IoT, αναφέρεται σε ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, ψηφιακών μηχανών και αντικειμένων ή οντοτήτων τα οποία χαρακτηρίζονται από μοναδικά αναγνωριστικά στοιχεία που τα ταυτοποιούν. Επιπρόσθετα, διακρίνονται από τη δυνατότητα ανταλλαγής πληροφοριών μέσω ενός δικτύου αλληλοεπιδρώντας μεταξύ ανθρώπων και μηχανών ή αντικειμένων ή χωρίς ανθρώπινη παρέμβαση η οποία περιλαμβάνει την αλληλεπίδραση αντικειμένου μεταξύ αντικειμένου. (Soro, et al., 2018) (Ullah, et al., 2017)[13, 37].

Η έννοια «πράγματα»[2] του όρου IoT, δεν συνδέεται αυστηρά με προϊόντα. Σχετίζεται με μία τεράστια γκάμα συσκευών οι οποίες διαφέρουν χαρακτηριστικά και λειτουργικά μεταξύ τους. Χαρακτηριστικό παράδειγμα είναι τα λεγόμενα «έξυπνα» αυτοκίνητα, τα οποία αποτελούν οχήματα με ενσωματωμένους αισθητήρες, κάμερες και κλιματιστικά, με προηγμένα συστήματα ασφαλείας κ.α., ακόμα και οχήματα τα οποία είναι εξοπλισμένα με αισθητήρες κίνησης, οι οποίοι εντοπίζουν αντικείμενα στην πορεία τους. Βασική προϋπόθεση αποτελεί η σύνδεση όλων των παραπάνω συσκευών μεταξύ τους, έτσι ώστε να υπάρχει η δυνατότητα από πλευράς χρήστη

[2] https://el.wikipedia.org

(καταναλωτή), να τα ελέγχει απομακρυσμένα από έναν κεντρικό υπολογιστή ή ακόμα και από ένα κινητό (2018-02-01) (Floerkemeier, et al., 2008)[11,47].

Πριν από μερικά χρόνια, ο όρος IoT θα μπορούσε να είναι ένα σενάριο επιστημονικής φαντασίας. Το να ζεσταίνεται το φαγητό στον φούρνο χωρίς την ανθρώπινη επίβλεψη, να ανοίγουν τα παραθυρόφυλλα του σπιτιού χωρίς την ανθρώπινη παρέμβαση και να παίζει η αγαπημένη μουσική αποτελούν χαρακτηριστικά παραδείγματα του όρου Διαδικτύου των Πραγμάτων. Η ρηξικέλευθη ανάπτυξη και διείσδυση του IoT στον τεχνολογικό κόσμο οφείλεται στην ανάπτυξη του λογισμικού (software), του υλικού (hardware), στην ανάπτυξη των τεχνολογιών των δικτύων, των λειτουργικών συστημάτων καθώς και στην ευκολία διασύνδεσης πλέον στο διαδίκτυο. Ουσιαστικά, πρόκειται για ένα πρότυπο νέας τεχνολογίας που αποσκοπεί στην δημιουργία ενός παγκόσμιου δικτύου μηχανών και συσκευών, που αποτελούνται από ενσωματωμένα ηλεκτρονικά συστήματα, αισθητήρες και λογισμικά που επιτρέπουν την συλλογή και την ανταλλαγή δεδομένων, ικανών να αλληλοεπιδρούν μεταξύ τους. Εναλλακτικές ονομασίες του, είναι «Διαδίκτυο των πάντων» ή μπορεί σπανίως να συναντηθεί και ως «Βιομηχανικό Διαδίκτυο». Οι διασυνδεδεμένες συσκευές ή μηχανές που χρησιμοποιούνται στην καθημερινή ζωή του ανθρώπου έχουν ως στόχο την αύξηση της αποτελεσματικότητας και της παραγωγικότητας του στις καθημερινές δραστηριότητες του.

Σήμερα πολλά εκατομμύρια απομακρυσμένες συσκευές, επικοινωνούν μεταξύ τους και συνδέονται αυτοματοποιημένα στο δίκτυο, για την εκτέλεση διάφορων εργασιών. Η δικτύωση των συσκευών τους προσδίδει μεγαλύτερη αποτελεσματικότητα και η υπηρεσία ή το αποτέλεσμα που παρέχεται χαρακτηρίζεται από μεγαλύτερη προστιθέμενη αξία για τους χρήστες. Θα υπάρχουν επενδύσεις σε μεγαλύτερη επεξεργαστική ισχύ, σε μεγαλύτερους αποθηκευτικούς χώρους καθώς και σε εκπαίδευση σε εργαλεία analytics. Στόχος των επενδύσεων είναι η βελτίωση της χρήσης των δεδομένων που λαμβάνονται από συσκευές συνδεδεμένες στο διαδίκτυο. Περίπου 6 τρισεκατομμύρια δολάρια υπολογίζονται οι επενδύσεις μέχρι το 2022 σε IoT. Υπολογίζεται ότι περίπου 13 τρισεκατομμύρια δολάρια θα επιφέρουν οι επενδύσεις σε IoT συσκευές έως το 2025. Μακροπρόθεσμα, το 2050 προβλέπεται ότι

θα επικοινωνούν και θα συνδέονται μεταξύ τους τουλάχιστον 50 δισεκατομμύρια συσκευές[3]. (Gubbi, και συν., 2013-09-01) (BI Intelligence, 2016)[7,19].

Λόγω της δικτυωμένης φύσης του σε συνδυασμό με την αυξανόμενη ευαισθησία των δεδομένων, εγείρονται πολλά ζητήματα όσον αφορά στην ασφάλεια και στην ακεραιότητα των δεδομένων που ανταλλάσσονται. Τα συστήματα λόγω της δημοτικότητάς τους σε διάφορους τομείς, όπως η ηλεκτρονική υγεία, το ηλεκτρονικό σπίτι και το ηλεκτρονικό εμπόριο, αποτελούν «στόχο» κακόβουλων ενεργειών από hackers/crackers, οι οποίοι θέτουν σε κίνδυνο την ασφάλεια και το απόρρητο τους. Πολλοί RFID readers εμπλέκονται στην ασφάλεια των IoT. Σε πολλά πρωτόκολλα αυθεντικοποίησης RFID για IoT υπάρχουν ανασφαλή κανάλια επικοινωνίας μεταξύ των reader και των back-end servers. Η ύπαρξη των μη ασφαλών καναλιών αποτελεί ευαίσθητο σημείο, διότι έχει σαν αποτέλεσμα πολλές RFID οντότητες να θεωρούνται μη αξιόπιστες. Έτσι, δημιουργείται η ανάγκη επινόησης νέων μηχανισμών ασφαλείας στα συστήματα IoT. Οι RFID ετικέτες καταγράφουν πληροφορίες, οι οποίες μπορεί να σχετίζονται με ευαίσθητα προσωπικά δεδομένα ή αλλιώς δεδομένα προσωπικού χαρακτήρα. Αυτό το γεγονός σε συνδυασμό με τα κενά ασφαλείας που προαναφέρθηκαν, δημιουργεί κινδύνους όσον αφορά στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων. Έτσι, τα κενά ασφαλείας των IoT συστημάτων, μαζί με εργαλεία που είναι διαθέσιμα σε hackers/crackers, καταστούν τα IoT συστήματα «πηγή διαρροής» ευαίσθητων προσωπικών δεδομένων. Επιπρόσθετα, ενδέχεται να αναπτυχθεί μια μορφή παρακολούθησης εις βάρος των χρηστών τους.

Συνεπώς, για να φτάσει το IoT στο μέγιστο των δυνατοτήτων του πρέπει να «θωρακιστεί» από ευπαθή σημεία που προκύπτουν. Από το 2016 έχει νομοθετηθεί η διαφύλαξη των προσωπικών δεδομένων στο IoT με το Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 (GDPR) (βλ. αναλυτικά Παράρτημα Α) αλλά και με γνωμοδοτήσεις και με σχετικές Ευρωπαϊκές οδηγίες. Κάποιες από τις σημαντικότερες ευπάθειες που τείνουν να απειλούν τα συστήματα IoT είναι οι μη ασφαλείς υπηρεσίες δικτύου που προαναφέρθηκαν, οι αδύναμοι δημόσιοι κωδικοί πρόσβασης, η έλλειψη κρυπτογράφησης και η κακή υποστήριξη ασφαλείας στα πλαίσια του υλικού από τις κατασκευαστικές εταιρίες. Στις συσκευές IoT

[3] https://www.operationscenter.eu/

διακρίνονται κάποια ιδιαίτερα χαρακτηριστικά σε επίπεδο υλικού (hardware) σε σχέση με το παραδοσιακό hardware. Τέτοια χαρακτηριστικά αφορούν στη συμβατότητα, την κατανάλωση ενέργειας, την κλιμάκωση, το μέγεθος των συσκευών και την προτυποποίηση. Αν και οι επεξεργαστές εξελίσσονται συνεχώς αυξάνοντας την απόδοσης τους, κρίνεται αναγκαία η χρήση συσκευών περιορισμένων δυνατοτήτων στα συστήματα IoT, δηλαδή συσκευών με περιορισμένη επεξεργαστική ισχύ, υπολογισμό και μνήμη και με αυστηρά περιορισμένη κατανάλωση ενέργειας. Τα ιδιαίτερα χαρακτηριστικά αυτά καθιστούν τα IoT επιρρεπή σε πολλές προηγμένες επιθέσεις και ζητήματα ασφαλείας που απαιτούν νέους μηχανισμούς ασφάλειας σε διαφορετικούς τομείς. Αντίμετρο σε επιθέσεις στα IoT αποτελούν οι PUF, οι οποίες έχουν αναδειχθεί ως μία πολλά υποσχόμενη ελαφριά εναλλακτική λύση ταυτότητας αντί της παραδοσιακής κρυπτογραφίας. Η λύση αυτή αφορά σε περιορισμένες συσκευές IoT. Οι συμβατικές υλοποιήσεις PUF έχουν βρεθεί ευάλωτες σε διαφορετικές επιθέσεις. Για τον λόγο αυτό, τα τελευταία χρόνια έχουν προταθεί διαφορετικά σχέδια PUF τα οποία έχουν μοντελοποιηθεί και αξιολογηθεί έναντι αυτών των επιθέσεων. Οι ειδικά σχεδιασμένες PUF για συσκευές IoT μπορούν να συμβάλλουν στην μείωση επιθέσεων και να αποτελέσουν λύσεις ασφάλειας.

1.2 ΒΑΣΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΤΟΥ IOT

Το IoT δεν χαρακτηρίζεται ως μία αυτοτελή τεχνολογία, αλλά μία ιδέα ανάπτυξης και συνδυασμός τεχνολογιών. Ιδιαίτερο γνώρισμα του Διαδικτύου των Πραγμάτων είναι η σταδιακά αυξημένη εισροή των μικρών υπολογιστικών συστημάτων και των τηλεπικοινωνιών, εντός του ανθρώπινου και φυσικού περιβάλλοντος, σε μεγαλύτερη πυκνότητα.

Η ανάπτυξη υπολογιστικών συστημάτων, όπου τα ψηφιακά «πράγματα» μπορούν να αλληλεπιδρούν με άλλα «πράγματα» για την ανταλλαγή και συλλογή δεδομένων, οδήγησε στην ανάγκη για εύρεση και συνδυασμό νέων τεχνολογιών. Οι νέες τεχνολογίες έχουν την δυνατότητα να καθιστούν δυνατή την επικοινωνία και τον εντοπισμό των «πραγμάτων» μεταξύ τους. Οι απαραίτητες τεχνολογίες υπάρχουν και συνεχίζουν να βελτιώνονται. Εκτός των «έξυπνων συσκευών», οι οποίες έχουν την

δυνατότητα να είναι συνδεδεμένες στο διαδίκτυο, αποτελεί απαίτηση και απαραίτητη προϋπόθεση η ενσωμάτωση τεχνολογιών, οι οποίες θα έχουν την δυνατότητα να συλλέγουν δεδομένα από το περιβάλλον, να αναγνωρίζουν τον τόπο του αντικειμένου και να συνδυάζουν τα δεδομένα αυτά με βέλτιστο τρόπο στο σχεδιασμό της γενικότερης αρχιτεκτονικής, έτσι ώστε να καταστεί δυνατή η υλοποίηση και η εφαρμογή της έννοιας του «Internet of Things». Όλα καθοδηγούνται από τις νέες δυνατότητες ψηφιακής ανίχνευσης, τα ενσωματωμένα συστήματα πληροφορικής και επικοινωνιών που συνδέονται μέσω RFID (αναγνώρισης συχνοτήτων), micro-chips, ασυρμάτων δικτύων αισθητήρων (WSN), QR (Quick Response) κωδικούς, barcodes, Wi-Fi, Bluetooth, Beacons, Analytics, Business Intelligence και Big Data. Νέες τεχνολογίες ασύρματης μετάδοσης πληροφοριών που έχουν αναπτυχθεί εξελίσσονται και μελετώνται από επιστημονικές κοινότητες συνεχώς. Κάποιες από τις τεχνολογίες αυτές έχουν δυνατότητα κάλυψης μεγάλων αποστάσεων, όπως το GPRS, LTE και LoRaWan, ενώ άλλες χαρακτηρίζονται από κάλυψη μικρότερων αποστάσεων για την δημιουργία τοπικών ασύρματων δικτύων, όπως το Wi-Fi, το Bluetooth, το ZigBee και το 6LoWPAN. Σημαντικές τεχνολογίες οι οποίες καθιστούν δυνατή την υλοποίηση του διαδίκτυο των πραγμάτων αποτελούν επίσης οι Sensors και τεχνολογία radio chip, τα οποία δίνουν την δυνατότητα στα «πράγματα» να αλληλοεπιδρούν με το περιβάλλον [21]. (Magrassi, 2001).

Το IoT, όπως δόθηκε από τον ορισμό, δεν είναι μία είναι τεχνολογία αλλά αποτελεί «μείγμα» διαφορετικών τεχνολογιών υλικολογισμικού. Το IoT δεν είναι απλά η επικοινωνία από μηχανή σε μηχανή (Machine to Machine), ασύρματα δίκτυα αισθητήρων, δίκτυα αισθητήρων, 2G/ 3G/ 4G, GSM, RFID, Wi-Fi, GPS, μικροελεγκτής και μικροεπεξεργαστής. Αυτά αποτελούν τεχνολογίες που καθιστούν δυνατή τη λειτουργία των IoT εφαρμογών. Οι τεχνολογίες στο IoT μπορούν να ομαδοποιηθούν σε τρείς κατηγορίες. Στην πρώτη κατηγορία συγκαταλέγονται τεχνολογίες που επιτρέπουν στα «πράγματα» να αποκτούν πληροφορίες. Η δεύτερη κατηγορία αφορά στην διαχείριση της πληροφορίας του «πράγματος». Η Τρίτη και τελευταία κατηγορία περιλαμβάνει τεχνολογίες που σχετίζονται με την βελτίωση της ασφάλειας και προστασίας της ιδιωτικής ζωής. Οι δύο πρώτες κατηγορίες είναι λειτουργικές και πρέπει να χαρακτηρίζονται από «νοημοσύνη», κάτι που διαφοροποιεί το IoT από το συνηθισμένο διαδίκτυο. Η Τρίτη κατηγορία τεχνολογιών

δεν αποτελεί λειτουργική κατηγορία, αλλά μία απαραίτητη προϋπόθεση στα πλαίσια της ασφάλειας.

1.2.1 RFID

Το RFID, η ταυτοποίηση μέσω ραδιοσυχνοτήτων, συχνά θεωρείται προαπαιτούμενο για το IoT. Θεμέλιο του internet of things αποτελεί η τεχνολογία ανίχνευσης της συσκευής. Το IoT χρησιμοποιεί ποικίλα είδη τεχνολογιών, που στέλνουν σήμα σε ένα ευρύ φάσμα συχνοτήτων, όπως η RFID. Η RFID tag αποτελεί ένα σύστημα, το οποίο ενσωματώνεται σε ένα αντικείμενο, εκπέμπει και λαμβάνει δεδομένα εκμεταλλευόμενη τα ραδιοκύματα με σκοπό την αναγνώριση και παρακολούθηση του αντικειμένου αυτού. Πρόκειται για την πιο βασική τεχνολογία του IoT όσον αφορά στην αναγνώριση, στον προσδιορισμό και στην σύνδεση των «πραγμάτων» [35]. (Ashton, 2009)

Η αναγνώριση ραδιοσυχνοτήτων χαρακτηρίζεται πλέον ως μία από τις πιο διαδεδομένες τεχνολογίες αυτόματης ταυτοποίησης που χρησιμοποιούνται. Οι τεχνολογίες τους ενσωματώνουν απλές συνιστώσες επικοινωνίας, καθώς και δυνατότητες Αποθήκευσης και υπολογισμών σε προσαρτημένες ετικέτες, οι οποίες έχουν την δυνατότητα να επικοινωνούν ασύρματα με απομακρυσμένους αναγνώστες. Παρέχουν ένα απλό και φθηνό τρόπο σύνδεσης φυσικών αντικειμένων στα πλαίσια του IoT, αφού κάθε αντικείμενο περιλαμβάνει μία ετικέτα (tag) παρέχοντας την δυνατότητα εντοπισμού και ταυτοποίησης (μέσω ραδιοκυμάτων) από τους αναγνώστες (readers). Πολυάριθμες εφαρμογές χρησιμοποιούν αυτές τις τεχνολογίες. Η παρακολούθηση προϊόντων, η μεταφορά προϊόντων και η αποπληρωμή των διοδίων σε αυτοκινητοδρόμους είναι ορισμένα παραδείγματα της τεχνολογίας αυτής [23,35]. (Chen, et al., 2016) (Ashton, 2009).

Το RFID σύστημα συνίσταται από ετικέτες ή αλλιώς αναμεταδότες, ένα πρόγραμμα ανάγνωσης και λογισμικό υποστήριξης. Ανάλογα με τον τύπο της εφαρμογής, οι συχνότητες RFID διαιρούνται σε τέσσερις διαφορετικές περιοχές συχνοτήτων. Στην περιοχή χαμηλής συχνότητας που κυμαίνεται στα 135 kHz ή και λιγότερο, στην περιοχή υψηλής συχνότητας που κυμαίνεται στα 13.56 MHz, στην

περιοχή Ultra-High συχνότητα που κυμαίνεται στα 862 MHz – 928 MHz και τέλος στην περιοχή συχνότητας μικροκυμάτων που κυμαίνεται στα 2.4 GHz.

Ένα RFID σύστημα απαρτίζεται από μεγάλο αριθμό ετικετών RFID, όπως προαναφέρθηκε. Περιλαμβάνουν έναν ή περισσότερους αναγνώστες (readers) RFID, καθώς και ένα διακομιστή back end. Οι ετικέτες ανάλογα με την λειτουργικότητα τους ταξινομούνται σε τρείς κατηγορίες: στις «παθητικές ετικέτες» τροφοδοτούμενες με ραδιοκύματα προερχόμενα από τον αναγνώστη RFID και επικοινωνούν μαζί του μέσω της λειτουργίας της ανάστροφης κατανομής. Δεύτερη κατηγορία είναι οι ετικέτες, οι οποίες τροφοδοτούνται μέσω των δικών τους πηγών ενέργειας, δηλαδή αυτόνομα και ονομάζονται «ενεργές ετικέτες» (ενεργητικές). Την τελευταία κατηγορία αποτελούν οι «ημι-ενεργές ετικέτες», οι οποίες κάνουν χρήση εσωτερικών πηγών ενέργειας για να τροφοδοτούν τα κυκλώματά τους, ενώ χρησιμοποιούν την λειτουργία της οπίσθιας σάρωσης για την επικοινωνία τους με τον αναγνώστη. Κατά βάση, η λειτουργικότητα της τεχνολογίας αυτής είναι λιτή και εύκολα κατανοητή [24]. (Finkenzeller, et al., 2010).

Παρόμοια λειτουργία με αυτή των RFID ετικετών αποτελεί αυτή των barcodes στα προϊόντα, κατά την οποία ένα scanner σαρώνει το barcode ενός προϊόντος και διαβάζει τις πληροφορίες σχετικές με αυτό. Η ειδοποιός διαφορά με τις ετικέτες RFID έγκειται στο γεγονός ότι το scanner έχει την δυνατότητα να διαβάσει μόνο ένα barcode την φορά και απαιτείται η οπτική επαφή μεταξύ τους, σε πολύ μικρή εμβέλεια. Αντιθέτως, οι RFID ετικέτες έχουν την δυνατότητα να διαβάσουν πολλά αναγνωριστικά την ίδια χρονική στιγμή, χωρίς να μπλέκονται και να δημιουργούν προβλήματα τα διάφορα σήματα των διαφορετικών ετικετών. Άλλη μία διαφορά σχετίζεται με την ανάγνωση τους, η οποία μπορεί να γίνει απομακρυσμένα χάριν στα ραδιοκύματα. Συγκεκριμένα, κάθε ετικέτα έχει μία μοναδική ταυτότητα ή αλλιώς ένα μοναδικό αναγνωριστικό (ID) που αναγνωρίζει ένα ορισμένο αντικείμενο, το οποίο είναι συνδεδεμένο, όπως ορίζεται από το πρωτόκολλο EPC Class-1 Gen-2. Αντικείμενο τέτοιο, μπορεί να είναι ένα όχημα, ένα ηλεκτρονικό διαβατήριο που περιέχει προσωπικές πληροφορίες, ένα προϊόν σε μια αποθήκη, μια συσκευή ιατρική που καταγράφει πληροφορίες στα πλαίσια της υγείας ενός νοσηλευόμενου ασθενούς ή οποιοδήποτε άλλη φυσική οντότητα διασυνδεδεμένη στο Διαδίκτυο. Ο πομποδέκτης κάθε ετικέτας, ο οποίος ενσωματώνεται σε ένα αντικείμενο επιτρέπει της μετάδοση και τη λήψη ραδιοσημάτων. Ως εκ τούτου, ένας αναγνώστης έχει την

δυνατότητα να επικοινωνεί με μία απομακρυσμένη ετικέτα, όσο η ετικέτα βρίσκεται στην περιοχή εμβέλειας της.

Η επικοινωνία μεταξύ των ετικετών RFID στα πλαίσια του IoT παρουσιάζουν προβλήματα λόγω της χαμηλής ισχύος μετάδοσης τους. Για να επιτραπεί η επικοινωνία μεταξύ τους απαιτείται ενίσχυση με τις αναδυόμενες ετικέτες δικτύου. Οι δικτυωμένες ετικέτες ή ετικέτες δικτύου, ενσωματώνονται με συστατικά συγκομιδής ενέργειας, τα οποία έχουν την δυνατότητα να συγκεντρώσουν ενέργεια από το περιβάλλον [23]. (Chen, et al., 2016).

Η εκμετάλλευση της τεχνολογίας RFID έδωσε νέες δυνατότητες σε διάφορους τομείς, σε οικονομικές δραστηριότητες και υπηρεσίες. Αυτό επιτυγχάνεται συνδέοντας αντικείμενα για την μεταβίβαση δεδομένων και δημιουργώντας την βάση των στοιχείων που επιτρέπει σε οργανισμούς να έχουν την δυνατότητα άμεσης πληροφόρησης από τις λειτουργικές διαδικασίες τους, ώστε να μπορούν σε διαρκή βάση και άμεσα να βελτιώσουν, να παρακολουθήσουν και να εξυπηρετήσουν σε ελάχιστο χρόνο τους πελάτες τους. Τα RFID αναπτύσσονται και εντάσσονται σε όλο και περισσότερους τομείς με τεράστια συνεισφορά. Η χρήση τους πλέον, διακρίνεται σε διάφορες δραστηριότητες των ανθρώπων, που σχετίζονται με τον αγροτικό τομέα, την ιατρική, τον αθλητισμό, μέχρι και την τεχνολογία σε στρατιωτικά συστήματα, που το απόρρητο είναι υψίστης σημασίας και σε δορυφορικά συστήματα. Επιπρόσθετα, η χρήση των ετικετών RFID έχει διαδραματίσει κομβικό ρόλο σε οργανισμούς αυξάνοντας θεαματικά την παραγωγικότητα τους, αφού έχει μειώσει δραματικά τα κόστη ορισμένων λειτουργιών, οι οποίες έως τότε ήταν κοστοβόρες ή απέτρεπαν την βελτίωση των υπηρεσιών τους [22,27]. (Roberti, October 2013) (Khattab, et al., 2017).

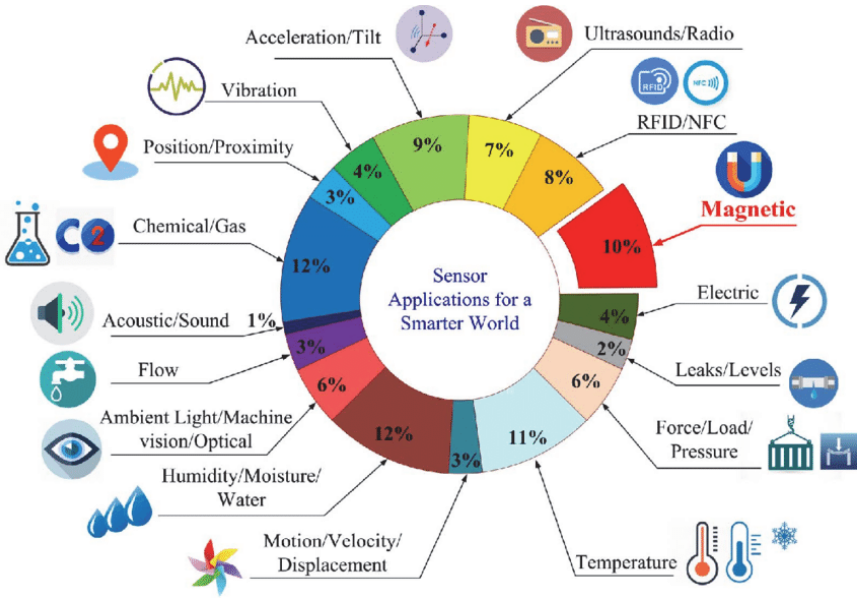
1.2.2 Αισθητήρες

Είναι ευρέως γνωστό ότι οι αισθητήρες αποτελούν μικρο-συσκευές, οι οποίες έχουν την δυνατότητα να μετρούν τις συνθήκες του εξωτερικού τους περιβάλλοντος στο οποίο τοποθετούνται και μετέπειτα να μεταφράζουν τη λαμβάνουσα πληροφορία.

Η πληροφορία μετατρέπεται σε ψηφιακή μορφή, ώστε να είναι απτή και να μπορεί να χρησιμοποιηθεί για παρατήρηση, για αξιολόγηση που σχετίζεται με τη ποιότητα του αντικειμένου και για χρήσιμες μετρήσεις. Ουσιαστικά, οι αισθητήρες αποτελούν συσκευές οι οποίες ενσωματώνονται σε άλλες συσκευές και τους επιτρέπουν να αλληλοεπιδρούν με το περιβάλλον. Δηλαδή, οι αισθητήρες ή τα «πράγματα» του συστήματος IoT αποτελούν την διεπαφή. Οι αισθητήρες συνδέονται άμεσα ή έμμεσα με δίκτυα IoT μετά από μετατροπή και επεξεργασία σήματος. Υπάρχει, πλέον, ένα ευρύ φάσμα αισθητήρων στο IoT που χρησιμοποιούνται για την ανίχνευση και την μέτρηση διάφορων φυσικών φαινομένων, όπως για παράδειγμα η θερμοκρασία και η πίεση, καθώς και οι πέντε ανθρώπινες αισθήσεις (όραση, αφή, ακοή, γεύση και μυρωδιά). Κύριος σκοπός των αισθητήρων είναι η συλλογή δεδομένων από το περιβάλλον [46,72]. (Gubbi, et al., September 2013) (Borgohain, et al., 2015)

Ένα σύστημα IoT αποτελείται από αισθητήρες/συσκευές που επικοινωνούν στο Cloud Computing (υπολογιστικού νέφους) μέσω κάποιου είδους συνδεσιμότητας. Μόλις τα δεδομένα φτάσουν στο Cloud, το λογισμικό τα επεξεργάζεται και ενδέχεται να εκτελέσει μία ενέργεια. Τέτοια ενέργεια μπορεί να είναι η αποστολή ειδοποίησης ή η αυτόματη προσαρμογή των αισθητήρων/συσκευών χωρίς την ανάγκη επέμβασης του χρήστη. Οι «έξυπνες συσκευές» προκειμένου να λειτουργήσουν σύμφωνα με το σχεδιαστικό τους πρότυπο, προϋποθέτουν την παραπάνω ενέργεια των αισθητήρων. Πρέπει ουσιαστικά, να διαβάζουν και να είναι σε αλληλεπίδραση με το περιβάλλον τους, έτσι ώστε να μπορούν να ανταποκρίνονται σε ερεθίσματα και να μπορούν να τα μεταφράζουν σε χρήσιμη πληροφορία ως προς των άνθρωπο [82]. (Genc, et al., 2015)

Παράδειγμα τέτοιο σήμερα, σχετικά με την λειτουργικότητα των αισθητήρων, αποτελούν οι «έξυπνοι» φούρνοι, οι οποίοι μπορούν να λειτουργούν από ένα κινητό τηλέφωνο δίνοντας τους την δυνατότητα να ψήνουν το φαγητό απομακρυσμένα χωρίς την φυσική παρουσία του νοικοκύρη ή της νοικοκυράς. Οι αισθητήρες είναι τεχνολογικό επίτευγμα που με κατάλληλο λογισμικό και υλικό, έχουν την δυνατότητα πλέον να ενσωματώνονται σε οικιακές συσκευές καθημερινής χρήσης και με τη δυνατότητα απομακρυσμένου χειρισμού να διευκολύνουν τους χρήστες στις καθημερινές τους δραστηριότητες [22,25]. (Roberti, October 2013) (Oreku, et al., 2016)



Εικόνα 2: Σύνολο εφαρμογών Αισθητήρων[4].

1.2.3 Bluetooth, Wi-Fi και Τεχνολογίες Δικτύωσης

Για την ανάπτυξη του IoT, σημαντικός παράγοντας αποτελεί η συνδεσιμότητα των συσκευών. Τα έξυπνα αντικείμενα IoT έχουν την δυνατότητα της αυτόνομης αλλαγής μιας συγκεκριμένης κατάστασης με ή χωρίς την ανθρώπινη παρέμβαση. Η ανάγκη για την ασύρματη επικοινωνία των συσκευών του IoT εξυπηρετείται από τις ασύρματες τεχνολογίες επικοινωνιών Z-wave, Zigbee, Wi-Fi, Bluetooth (BLE), την κινητή επικοινωνία 4G/5G, Insteon, πρότυπο IEEE 802.15.6 και άλλες τεχνολογίες βασισμένες σε πρότυπα IEEE [26]. (Rockerhousen, 2016)

Το Bluetooth (BLE, Bluetooth χαμηλής ενέργειας) είναι μία ασύρματη τεχνολογία επικοινωνίας με παρουσία πριν από το Internet of Things. Αποτελεί έναν αξιόπιστο και συμβατό τρόπο συνδεσιμότητας όλων των συσκευών. Η τεχνολογία Bluetooth βελτιώνει την γενική λειτουργικότητα των «έξυπνων» συσκευών. Το Bluetooth χρησιμοποιεί μερικές διαφορετικές τοπολογίες δικτύου.

[4] https://www.researchgate.net

Η πιο συνηθισμένη είναι η piconets τοπολογία από σημείο σε σημείο που μπορούν να συμμετέχουν δύο έως οκτώ στο ίδιο κανάλι, συνδεδεμένες συσκευές Bluetooth. Το Bluetooth επιτρέπει σε κάθε κόμβο να συμμετέχει στην επεξεργασία δεδομένων με οποιοδήποτε άλλο κόμβο του δικτύου, χάρη στην τοπολογία δικτύου πλέγματος. Με τα δίκτυα πλέγματος μια συσκευή που είναι απομονωμένη έχει την δυνατότητα να επικοινωνεί, ανεξάρτητα από το αν μια συσκευή έχει αποσυνδεθεί. Χαρακτηρίζεται από υψηλές ταχύτητες επικοινωνίας για μεγάλο χρονικό διάστημα, με μικρές πηγές ενέργειας και έχει στην διάθεση του μεγάλο εύρος σημάτων. Η ανταλλαγή δεδομένων πραγματοποιείται σε μικρή εμβέλεια κάνοντας χρήση της ακτινοβολίας UHF μικρού μήκους κύματος και έχει την δυνατότητα να εγκατασταθεί σε κινητές και σταθερές συσκευές με σκοπό την πραγματοποίηση προσωπικών δικτύων (PAN). Η ανάγκη για την μείωση της απαιτούμενης ενέργειας προκύπτει από το γεγονός ότι για τις λειτουργίες του Διαδικτύου των πραγμάτων η χρήση του διαδικτύου και η παραδοσιακή τεχνολογία μπορεί να βλάψει την μπαταρία των συσκευών του IoT, μειώνοντας τον χρόνο ζωής της.

Μία ευρέως γνωστή πλέον τεχνολογία ασύρματης επικοινωνίας συντελεί το Wi-Fi. Το όραμα του IoT δεν απαιτεί μόνο την σύνδεση με οικιακές συσκευές της καθημερινής ζωής και με καταναλωτικές ηλεκτρονικές συσκευές, αλλά απαιτεί και σύνδεση με μπαταρίες που δεν μπορούν να επαναφορτιστούν. Συχνά, ενσωματώνονται σε μπαταρίες διάφοροι τύποι ενεργοποιητών και αισθητήρων, οι οποίοι απαιτούνται για την διατήρηση της αξιόπιστης λειτουργίας συσκευών για πολλά χρόνια. Το πρότυπο IEEE 802.11 χρησιμοποιείται σε τοπικά δίκτυα WLAN, με στόχο την ασύρματη σύνδεση χρηστών με τερματικές συσκευές. Με βάση όλων των πρότυπων IEEE 802.11 δημιουργήθηκε το Wi-Fi Alliance, που συνιστά μία επέκταση του γνωστού Wi-Fi, με στόχο την καλύτερη λειτουργία κάθε τοπικού δικτύου WLAN. Αναλόγως, κυκλοφόρησαν και άλλες προδιαγραφές στο πρότυπο IEEE 802.11 (IEEE 802.11.a, IEEE 802.11.b, IEEE 802.11.g, IEEE 802.11.ac), τα οποία διαφέρουν στο εύρος ζώνης και στον ρυθμό μετάδοσης. Η επαναχρησιμοποίηση της υπάρχουσας υποδομής Wi-Fi παρέχει εξοικονόμηση κόστους και συνδράμει στην ταχύτερη ανάπτυξη τεχνολογιών. Πλεονέκτημα για το IoT, αποτελεί η εγγενή συμβατότητα δικτύου IP, η διαθεσιμότητα εργαλείων διαχείρισης δικτύου και γνωσιακής βάσης, καθώς

υπάρχει εξοικείωση για την διαχείριση δικτύων Wi-Fi, η αύξηση της διάρκειας της μπαταρίας και τέλος η βελτίωση του συνολικού κόστους ιδιοκτησίας [33]. (Panicker, 2020).

Το ZigBee βασίζεται στο πρότυπο IEEE 802.15.4. Λόγω του ενεργειακά αποδοτικού σχεδιασμού του, λαμβάνεται υπόψη για εφαρμογές δικτύου αισθητήρων. Η τεχνολογία του εφαρμόζεται σε πολλούς κλάδους (υγειονομική περίθαλψη, συστήματα ασφαλείας κτλ.). Αποτελεί ένα από τα πιο αξιόπιστα πρωτόκολλα στον κόσμο των ασύρματων δικτύων. Διακρίνεται από χαμηλή κατανάλωση ενέργειας, κάτι που το καθιστά οικονομικό και αποδοτικό. Είναι πρωτόκολλο μικρής εμβέλειας και λόγω αυτού βρίσκεται σε συσκευές IoT με εμβέλεια μικρότερη των εκατό μέτρων, ελέγχοντας απλές συσκευές. Παραδείγματα των παραπάνω συσκευών είναι οι θερμοστάτες και τα LEDs. Σε μία τεχνολογία ZigBee υπάρχουν τρείς τύποι τοπολογίες. Η τοπολογία πλέγματος, όπου κάθε τερματική συσκευή μπορεί να επικοινωνήσει με οποιαδήποτε συσκευή ίδιας εμβέλειας. Οι συσκευές Full-Function (συσκευές είναι μονίμως ενεργοποιημένες άρα έχουν και υψηλή κατανάλωση ενέργειας) λειτουργούν ως δρομολογητές ή ως συντονιστές και οι συσκευές Reduced-Function (συσκευές λειτουργούν σε αναστολή άρα προσφέρουν εξοικονόμηση ενέργειας) λειτουργούν ως τερματικές συσκευές. Άλλου είδους τοπολογία είναι η τοπολογία αστέρα, κατά την οποία υπάρχει συντονιστής και τερματικές συσκευές και είναι υπεύθυνη για την μεταφορά δεδομένων. Τέλος, σε μία τεχνολογία ZigBee υπάρχει και η τοπολογία Cluster Tree, όπου οι τερματικές συσκευές συνδέονται με έναν συντονιστή και δεν υπάρχει η δυνατότητα να επικοινωνούν άμεσα με άλλες τερματικές συσκευές.

Το 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) αναπτύχθηκε για να καλύψει IP για συγκεκριμένες ανάγκες των ασύρματων αισθητήρων. Βασίστηκε στο πρότυπο IEEE 802.15.4. Για την δρομολόγηση των πακέτων δεδομένων κάνει χρήση της IPv6 τεχνολογίας. Για τα συστήματα IoT η τεχνολογία 6LoWPAN αντιμετωπίζει επάξια το πρόβλημα συνδεσιμότητας πλήθους συσκευών (επεκτασιμότητα). Λειτουργεί σε συσκευές με χαμηλή ισχύ με αποτέλεσμα την εξοικονόμηση ενέργειας. Η τεχνολογία 6LoWPAN παρέχει δυνατότητα κρυπτογράφησης και ελέγχου ταυτότητας χρησιμοποιώντας το

σύστημα ασφαλείας AES-128. Ως εκ τούτου, χαρακτηρίζεται μία ασφαλή τεχνολογία με δυνατότητα κλιμάκωσης του δικτύου [32]. (Patel, et al., May 2016)

Η τεχνολογία Insteon είναι μία τεχνολογία οικιακού αυτοματισμού. Χρησιμοποιεί τοπολογία δικτύωσης διπλού πλέγματος στην οποία όλες οι συσκευές είναι ομότιμες και κάθε συσκευή μεταδίδει και λαμβάνει ανεξάρτητα μηνύματα. Είναι πρωτόκολλο εύκολης λειτουργίας, καθώς οι συσκευές Insteon συνδέονται στο διαδίκτυο αυτόματα με την ενεργοποίησή τους. Χαρακτηρίζεται από μεγάλη επεκτασιμότητα και συμβατότητα συσκευών.

Το Z-Wave είναι ένα πρωτόκολλο ασύρματων επικοινωνιών που χρησιμοποιείται κυρίως στα πλαίσια του οικιακού αυτοματισμού, όπως και η προαναφερθείσα τεχνολογία Insteon. Είναι ένα δίκτυο πλέγματος που λειτουργεί με εύρος συχνότητας της τάξεως των 908,42 MHz. Επιτρέπει τον ασύρματο έλεγχο καθημερινών «έξυπνων» οικιακών συσκευών. Ένα Z-Wave έχει την δυνατότητα να ελεγχθεί μέσω διαδικτύου απομακρυσμένα μέσω ενός «έξυπνου» κινητού τηλεφώνου ή από υπολογιστή, καθώς και τοπικά από συσκευές, όπως ασύρματο πληκτρολόγιο, «έξυπνο» ηχείο κ.α. Παρέχει εξοικονόμηση ενέργειας, υψηλό ρυθμό μετάδοσης δεδομένων καθώς και συμβατότητα πλήθους συσκευών. Υπάρχει ένας αυξανόμενος αριθμός διαλειτουργικών προϊόντων Z-Wave, σύμφωνα με μελέτες, συγκεκριμένα πάνω από 1.700 κατά τη χρονιά 2007 και πάνω από 2.600 το 2019.

1.2.4 Cloud Computing

Το Cloud Computing συνιστά τάση τελευταίων χρόνων στον τομέα της πληροφορικής. Η χρήση του υπολογιστικού νέφους «λύνει τα χέρια» των χρηστών του, όσον αφορά στην ανησυχία περί συντήρησης και διαχείρισης των πόρων. Αποτελεί ένα δικτυακό μοντέλο Αποθήκευσης δεδομένων, κατά το οποίο η Αποθήκευση τους πραγματοποιείται σε απομακρυσμένες δικτυακές τοποθεσίες. Ο χρήστης επιβαρύνεται με το σχετικό κόστος των υπηρεσιών γνωστό ως «pay as you use». Αναλυτικότερα, οι πληροφορίες αποθηκεύονται σε τεράστια σε μνήμη κέντρα

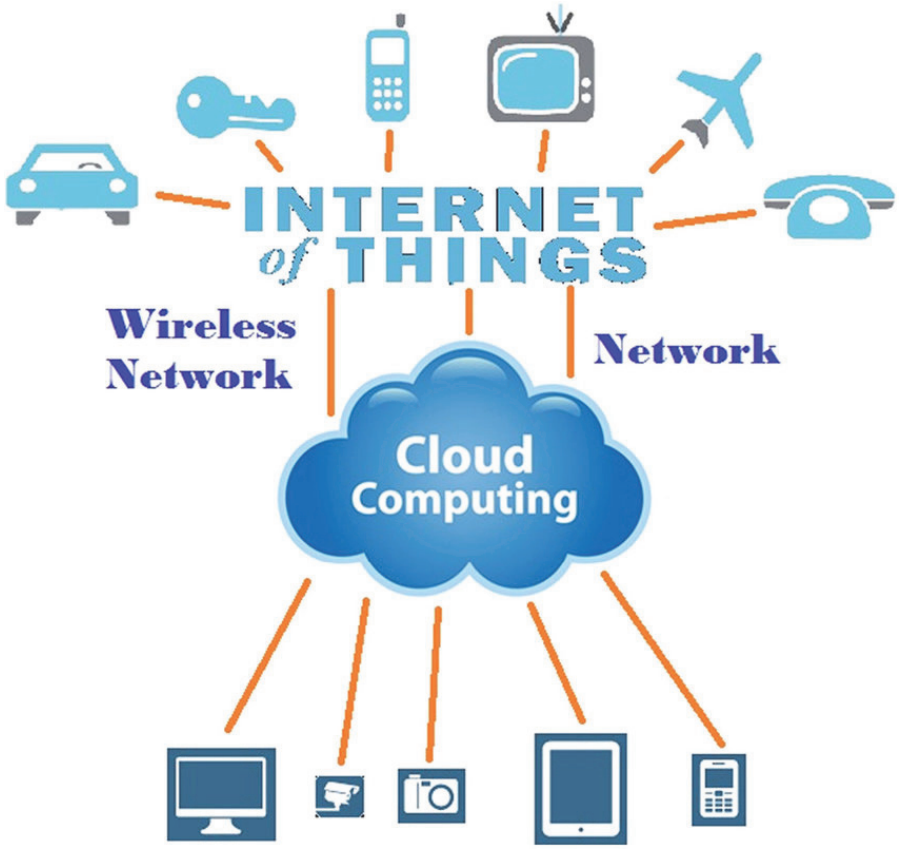
Αποθήκευσης δεδομένων (data centers), τα οποία μπορεί να εντοπίζονται σε έναν εξυπηρετητή ή διασκορπισμένα σε περισσότερους εξυπηρετητές, βάσει της κατανεμημένης ιδιότητας που χαρακτηρίζει την τεχνολογία. Η πρόσβαση στα δεδομένα από τον χρήστη πραγματοποιείται μέσω κάποιας δικτυακής διεπαφής (web interface). Με την «έξυπνη» τεχνολογία του υπολογιστικού νέφους πραγματοποιείται η πρόσβαση στα πράγματα οποιαδήποτε στιγμή και από οποιοδήποτε μέρος. Αποτελεί, ίσως, το πιο σημαντικό μέρος του IoT, επειδή δεν συνδέει απλά τους διακομιστές, αλλά αναλύει και τα χρήσιμα δεδομένα που λαμβάνονται από τους αισθητήρες και παράλληλα παρέχει πολλούς πόρους για την Αποθήκευση των δεδομένων (μετρήσεων). Έτσι, η τεχνολογία αυτή μπορεί να μετατρέψει ένα smartphone σε ένα μεγάλο κέντρο δεδομένων [45]. (Botta, 2016).

Η έννοια του «υπολογιστικού νέφους» σχετίζεται με υπηρεσίες και εφαρμογές, οι οποίες βρίσκονται σε κατανεμημένο δίκτυο. Η πρόσβαση σε αυτές, πραγματοποιείται μέσω κοινών πρωτοκόλλων του διαδικτύου και προτύπων δικτύωσης. Σχετικοί οργανισμοί είναι υπεύθυνοι για την παροχή των υπηρεσιών αυτών, οι οποίοι διακρίνονται για τη διάθεση μεγάλων χώρων Αποθήκευσης. Τους αποθηκευτικούς πόρους του υπολογιστικού νέφους μπορούν να εκμεταλλευτούν χρήστες ανεβάζοντας αρχεία χωρίς να καταναλώνουν δικούς του πόρους και να αποκτούν πρόσβαση σε αρχεία μέσω μίας απλής σύνδεσης. Με την ανάπτυξη διαδικτύου (Internet) ή αλλιώς του παγκόσμιου δικτύου, ο κάθε χρήστης του πλέον, έχει την δυνατότητα να συνδεθεί σε αυτό, από οποιοδήποτε τόπο σε ολόκληρο τον κόσμο, οποιαδήποτε χρονική στιγμή και σε οποιαδήποτε υπηρεσία, που προσφέρει online προγράμματα ή προσφέρει αποθηκευτικούς χώρους [29,45,82]. (Mavromoustakis, et al., 2017) (Botta, 2016) (Genc, et al., 2015)

Υπάρχουν και αντίστοιχα μοντέλα παροχής υπηρεσιών που προσφέρουν διαφορετικές δυνατότητες. Τα βασικότερα μοντέλα είναι το SaaS (Software as a Service), το PaaS (Platform as a Service), το NaaS (Networks as a Service) και το IaaS (Infrastructure as a Service). Το λογισμικό ως υπηρεσία (SaaS) παρέχει την δυνατότητα στον χρήστη να έχει πρόσβαση σε εφαρμογή χωρίς να είναι απαραίτητη η Αποθήκευση, η εγκατάσταση και η συντήρηση της εφαρμογής. Η εφαρμογή είναι διαθέσιμη και λειτουργεί μετά από την πληρωμή της από τον καταναλωτή μέσω διαδικτύου. Χαρακτηριστικό παράδειγμα αποτελεί το Google Drive και οι εφαρμογές του, οι οποίες είναι άμεσα διαθέσιμες και μπορούν να τρέξουν απ' ευθείας online.

Η τεχνολογία του υπολογιστικού νέφους επέφερε τεράστιες αλλαγές στο τρόπο συλλογής και Αποθήκευσης δεδομένων συγκριτικά με το παραδοσιακό μοντέλο. Η ένταξη των υπηρεσιών cloud computing σε επιχειρήσεις και οργανισμούς συνδυάστηκε με πλεονεκτήματα, όσον αφορά στο κόστος, την ταχύτητα, την αξιοπιστία και την παραγωγικότητα τους. Τα πλεονεκτήματα αυτά έχουν οδηγήσει όλο ένα και πιο πολλές επιχειρήσεις στις υπηρεσίες του. Με την χρήση των υπηρεσιών του εξαλείφεται το κόστος κεφαλαίου για την αγορά υλικολογισμικού, καθώς και η δημιουργία και λειτουργία κέντρων δεδομένων που χαρακτηρίζονται από υψηλό κόστος. Οι υπολογιστικοί πόροι παρέχονται κατ' απαίτηση με αποτέλεσμα να μπορούν να διατίθενται σε αμελητέο χρονικό διάστημα. Με την τεχνολογία του υπολογιστικού νέφους η δημιουργία αντιγράφων ασφαλείας των δεδομένων και η αποκατάσταση καταστροφών είναι λιγότερο κοστοβόρα και πραγματοποιείται ευκολότερα. Τέλος, το Cloud computing εξαλείφει την ανάγκη για συνεχείς ρυθμίσεις, συντήρηση, εγκατάσταση λογισμικού και επιδιόρθωση λογισμικού με αποτέλεσμα να αυξάνει την παραγωγικότητα της επιχείρησης ή του οργανισμού [30]. (LeadingEdge).

Παρά την θετική συνεισφορά της τεχνολογίας του Cloud computing, εμφανίζεται το πρόβλημα της ασφάλειας των δεδομένων. Αν και διαθέτει προηγμένα συστήματα προστασίας κατά των επιθέσεων, υπάρχει ο κίνδυνος να κλαπούν από κακόβουλους χρήστες που είτε επιδιώκουν κέρδος είτε αποσκοπούν σε προσωπική ευχαρίστηση. Επιπρόσθετα, το υπολογιστικό νέφος αποτελεί πηγή εκμετάλλευσης για κακόβουλους χρήστες, αφού μπορούν εύκολα να αποθηκεύουν ενοχοποιητικά αρχεία στο περιβάλλον του σε αποθηκευτικούς χώρους. Στους χώρους Αποθήκευσης δεδομένων, οι υπηρεσίες ελέγχου και οι υπηρεσίες επιβολής νόμου αποκτούν πολύ δύσκολα πρόσβαση σε ενοχοποιητικά αρχεία κακόβουλων χρηστών, καθώς λόγω της κατανεμημένης φύσης του μπορεί τα αρχεία αυτά να έχουν αποθηκευτεί σε οποιαδήποτε τόπο, ο οποίος φιλοξενεί τους κεντρικούς υπολογιστές των εταιρειών υπολογιστικού νέφους. (Mavromoustakis, et al., 2017) (Stergiou, et al., 2016)[14,70].



Εικόνα 3: Ενσωμάτωση Cloud Computing στο IoT[5].

1.3 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ IOT

Το IoT αποτελεί ένα σύνθετο σύστημα πολλών συνδεδεμένων συσκευών με διάφορα χαρακτηριστικά. Τα πιο βασικά χαρακτηριστικά εν' συντομία είναι τα εξής. (Patel, et al., May 2016) (Vermesan, et al., 2013) [15,16,32]:

- **Συνδεσιμότητα:** Το χαρακτηριστικό αυτό συντελεί ίσως το πιο σημαντικό χαρακτηριστικό του IoT. Χωρίς τη συνδεσιμότητα δεν υφίσταται επικοινωνία μεταξύ των συσκευών του

[5] https://www.researchgate.net/publication/311065854_Secure_Integration_of_Internet-of-Things_and_Cloud_Computing

διαδικτύου των πραγμάτων. Οι συσκευές IoT έχουν την δυνατότητα να συνδεθούν μέσω ραδιοκυμάτων, Wi-Fi, Li-Fi ,Bluetooth κ.λπ. Το IoT επίσης, έχει την δυνατότητα σύνδεσης σε ένα παγκόσμιο σύστημα πληροφορικής και τηλεπικοινωνιών.

- **Ασφάλεια:** Σχετίζεται με την προστασία των προσωπικών δεδομένων. Αποτελεί ένα από τα κύρια χαρακτηριστικά του Διαδικτύου των πραγμάτων. Με τον συνεχώς αυξανόμενο αριθμό συνδεδεμένων συσκευών IoT στο διαδίκτυο αυξάνεται και η ανάγκη για ασφάλεια των δεδομένων. Κατά την σχεδίαση του IoT απαιτούνται μέτρα ασφαλείας και τείχη προστασίας για την αποτροπή χειραγώγησης και κακής χρήσης των δεδομένων.
- **Νοημοσύνη:** Σήμερα, στην πληθώρα των περιπτώσεων όπου χρησιμοποιείται το IoT, τα δεδομένα, χρησιμοποιούνται για τη λήψη σημαντικών επιχειρηματικών πληροφοριών και την προώθηση σημαντικών επιχειρηματικών αποφάσεων. Η συνδρομή της τεχνητής νοημοσύνης στο IoT αφορά στην αλληλεπίδραση μεταξύ συσκευών, έτσι ώστε να προσαρμόζονται και να πραγματοποιούν αυτόματα καθορισμένες λειτουργίες. Η προσαρμοστικότητα και η πραγματοποίηση αυτόματα καθορισμένων λειτουργιών οφείλονται στην εκπαίδευση μέσω της μηχανικής μάθησης.
- **Κλιμάκωση:** Ο αριθμός των συνδεδεμένων συσκευών οφείλει να είναι πολλαπλά μεγαλύτερος σε μέγεθος από τις συσκευές που είναι συνδεδεμένες στο τρέχον Διαδίκτυο. Οι συσκευές IoT είναι απαραίτητο να είναι σχεδιασμένες κατά τρόπο τέτοιο, ώστε να έχουν την δυνατότητα να κλιμακώνονται ή να αυξάνονται με ευκολία.
- **Δυναμικές αλλαγές:** Η κατάσταση των συσκευών καθώς και ο αριθμός τους μπορεί να αλλάζει δυναμικά. Η κατάσταση μίας συσκευής μπορεί να αλλάξει δυναμικά την κατάσταση της από

«ύπνος» σε «αφύπνιση», να συνδεθεί ή να αποσυνδεθεί ανάλογα με την θερμοκρασία, την θέση και την ταχύτητα.

- **Αίσθηση/Ανίχνευση:** Στο IoT υπάρχει ανάγκη για την μετατροπή του αναλογικού σήματος με σκοπό την άντληση σημαντικών πληροφοριών και γνώσεων από το σήμα. Η συλλογή των δεδομένων πραγματοποιείται με χρήση RFID, GPS, αισθητήρων κ.λπ.. Οι τεχνολογίες ανίχνευσης του IoT, ουσιαστικά, επιτρέπουν στις συσκευές του Διαδικτύου των Πραγμάτων να τροποποιούνται ανάλογα με την κατάσταση του περιβάλλοντος.
- **Ετερογένεια:** Αποτελεί βασικό χαρακτηριστικό στο Internet of Things. Οι συσκευές IoT είναι βασισμένες σε διαφορετικά δίκτυα (πρωτόκολλα επικοινωνίας) και διαφορετικές πλατφόρμες. Οι συσκευές έχουν την δυνατότητα να αλληλοεπιδρούν με άλλες συσκευές ή με άλλες πλατφόρμες υπηρεσιών. Η αλληλεπίδραση μπορεί να γίνει μέσω διαφορετικών δικτύων. Βασικές απαιτήσεις για ετερογενή πράγματα συντελεί η επεκτασιμότητα και η δια-λειτουργικότητα.

1.4 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΙΟΤ

Η αρχιτεκτονική του IoT απαρτίζεται από διαφορετικά επίπεδα τεχνολογιών για την υποστήριξη της λειτουργικότητας του. Οι εφαρμογές του διαδικτύου των πραγμάτων βασίζονται σε αποσπασματικές εφαρμογές λογισμικού για συγκεκριμένα συστήματα και περιπτώσεις χρήσης. Αν και κάθε σύστημα IoT είναι διαφορετικό η αρχιτεκτονική παραμένει η ίδια.

Τα επίπεδα της αρχιτεκτονικής του IoT είναι το επίπεδο ανίχνευσης ή αλλιώς επίπεδο αισθητήρα, το επίπεδο δικτύου και πυλών, το επίπεδο διαχείρισης υπηρεσίας ή αλλιώς το επίπεδο ανάλυσης και τέλος το επίπεδο εφαρμογής [15,17].

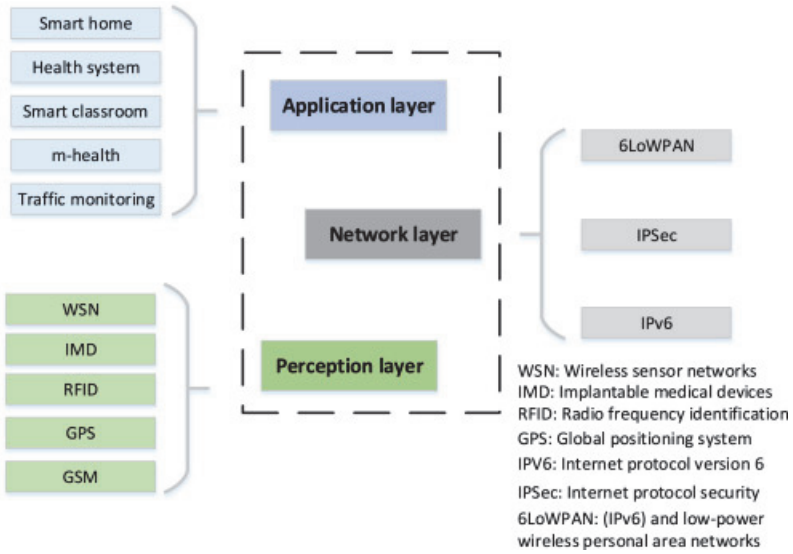
Το sensor layer (επίπεδο ανίχνευσης) είναι το χαμηλότερο επίπεδο και περιλαμβάνει συσκευές ανίχνευσης, ασύρματα δίκτυα αισθητήρων, ενεργοποιητές, ελεγκτές, και ετικέτες ραδιοσυχνοτήτων RFID. Οι αισθητήρες επιτρέπουν τη διασύνδεση ψηφιακού και φυσικού κόσμου, επιτρέποντας πληροφορίες να συλλέγονται και να ανταλλάσσονται σε πραγματικό χρόνο. Η μεταβιβάσιμη πληροφορία, προκύπτει από την λήψη μετρήσεων συνθηκών του περιβάλλοντος. Η θερμοκρασία, ταχύτητα, υγρασία, κίνηση, κτλ. αποτελούν μεταβολή των συνθηκών του περιβάλλοντος, όντας πληροφορία που ο αισθητήρας συλλέγει και υποβάλλει. Με βάση τα δεδομένα που ανιχνεύονται σε πραγματικό χρόνο από τους αισθητήρες, το σύστημα αναλύει και δίνει εντολές στους ενεργοποιητές να ενεργήσουν για κάποια συγκεκριμένη κατάσταση. Οι αισθητήρες ομαδοποιούνται βάσει του σκοπού τους (π.χ. αισθητήρες οικιακών συσκευών). Οι συσκευές με δίκτυα μικρής εμβέλειας και οι κόμβοι αισθητήρων του επιπέδου ανίχνευσης έχουν περιορισμένη ισχύ. Λόγω του τεράστιου πλήθους των πληροφοριών αλλά και του χώρου που απαιτείται να καλυφθεί για αυτές τις πληροφορίες, χρειάζονται πολλαπλοί κόμβοι και ένα αυτό-οργανωμένο σύστημα. Ενδεικτικά πρωτόκολλα για την διαχείριση του πλήθους των συσκευών του IoT αποτελούν το M2M και το WSN, τα οποία φιλοξενούν πληθώρα κόμβων αισθητήρα και είναι αποτελεσματικά για χρήση συσκευών χαμηλής ισχύος, καλύπτοντας μεγάλες περιοχές και διατηρώντας επαρκή την διάρκεια ζωής της μπαταρίας.

Το Network and Gateways Layer (επίπεδο δικτύου) συγκροτεί το επίπεδο που δίνει πρόσβαση στο διαδίκτυο και είναι αρμόδιο για την μετάδοση και επεξεργασία των δεδομένων. Από τους αισθητήρες προκύπτει τεράστιος όγκος δεδομένων, γεγονός που απαιτεί ενσύρματο ή ασύρματο δίκτυο υψηλής απόδοσης, που θα αποτελεί το μέσο μεταφοράς αυτών των δεδομένων. Το επίπεδο αυτό χρησιμοποιεί συνήθως συσκευές που έχουν δυνατότητα προσπέλασης σε ετερογενή δίκτυα, τα οποία προσφέρουν μια ομοιογενή ευρυζωνική πρόσβαση ανεξαρτήτως θέσης στο δίκτυο. Στο συγκεκριμένο επίπεδο, την μεγαλύτερη λειτουργικότητα την έχουν οι πύλες (gateways). Οι πύλες χαρακτηρίζονται από υλικό και λογισμικό. Συναντώνται διάφορες πύλες, όπως για παράδειγμα μικροεπεξεργαστής και μικροελεγκτής, καθώς και διάφορα

δίκτυα πυλών, όπως GSM και το Wi-Fi. Η επεξεργασία και η αξιοποίηση της επεξεργάσιμης πληροφορίας μπορεί να γίνει από τις πύλες.

Το Analysis Layer ή Management Service Layer (επίπεδο υπηρεσιών) είναι το πιο γρήγορο επίπεδο επεξεργασίας πληροφοριών, το οποίο επιτυγχάνεται μέσω αναλυτικών στοιχείων. Το IoT χαρακτηρίζεται από την σύνδεση και την αλληλεπίδραση αντικειμένων και συστημάτων σε συνδυασμό με την παροχή πληροφοριών ανάμεσα τους με την μορφή συμβάντων ή δεδομένων που σχετίζονται με την θερμοκρασία, την κίνηση, την τοποθεσία, κτλ. Η επεξεργασία των πληροφοριών γίνεται με υψηλή ταχύτητα σε πραγματικό χρόνο. Το επίπεδο υπηρεσιών, προσφέρει υπηρεσίες σε εφαρμογές μεγάλης κλίμακας. Στον τομέα των αναλυτικών στοιχείων, χρησιμοποιούνται διάφορα εργαλεία ανάλυσης, τα οποία εξάγουν τις σχετικές πληροφορίες από των τεράστιο όγκο δεδομένων. Πέρα των συστημάτων ανάλυσης και εξαγωγής δεδομένων που περιλαμβάνει το επίπεδο αυτό, περιλαμβάνει, επίσης, και συστήματα υπολογιστικού νέφους, υπολογιστικά συστήματα μαζικής Αποθήκευσης δεδομένων, καθώς και γεωγραφικά πληροφοριακά συστήματα που σχετίζονται με την επιστήμη της γεωλογίας και γεωπεριβάλλοντος. Στο επίπεδο της ανάλυσης περιλαμβάνονται και τεχνικές «φιλτραρίσματος» των δεδομένων, όπως ενοποίηση δεδομένων, ανωνυμοποίηση δεδομένων και συγχρονισμός δεδομένων που χρησιμοποιούνται για την απόκρυψη των λεπτομερειών των πληροφοριών κατά την παροχή τους.

Στο Application Layer περιλαμβάνονται οι πλατφόρμες IoT, οι οποίες ενεργοποιούν τις εφαρμογές IoT παρέχοντας μια γρήγορη απόκριση των υπηρεσιών. Οι εφαρμογές αφορούν τομείς, όπως αυτόν των μεταφορών, της «έξυπνης» πόλης, της αλληλεπίδρασης χρηστών, της υγειονομικής περίθαλψης, της ενέργειας και άλλους τομείς. Οι συσκευές του διαδικτύου των πραγμάτων έχουν αξιόλογη συνεισφορά στους παραπάνω τομείς, βελτιώνοντας και διευκολύνοντας την καθημερινότητα των ανθρώπων [31,69]. (Ullah, et al., 2017) (Shamsoshoara, και συν., 2020).



Εικόνα 4: Δομή Διαδικτύου των Πραγμάτων[6].

[6] https://www.sciencedirect.com/

ΚΕΦΑΛΑΙΟ 2 : ΑΣΦΑΛΕΙΑ ΣΤΟ INTERNET OF THINGS

Με τη καθολική χρήση του διαδικτύου προέκυψαν ζητήματα όσον αφορά στην ασφάλεια δεδομένων. Παρά τις σημαντικές επενδύσεις στον τομέα της ασφάλειας των πληροφοριακών συστημάτων, προηγμένες ικανότητες κακόβουλων ατόμων σε συνδυασμό με εξειδικευμένα εργαλεία που έχουν στην διάθεση τους αποτελούν πηγή κινδύνου. Επιτιθέμενοι εκμεταλλεύονται τα διαθέσιμα εργαλεία και τις ικανότητες τους έχοντας ως στόχο την απόκτηση πληροφοριών. Στα συστήματα IoT, οι συσκευές που το απαρτίζουν δημιουργούν ακούσια μεγάλο αριθμό ευαίσθητων δεδομένων, τα οποία δεδομένα αφορούν στην καθημερινότητα του ανθρώπου, αφού οι συσκευές μπορεί να λαμβάνουν τόπο είτε στο σπίτι του (π.χ. κάμερες ασφαλείας), είτε ακόμα και για την παρακολούθηση της υγείας του.

Η ανταλλαγή δεδομένων μεταξύ συνδεδεμένων συσκευών του IoT καθιστά τις μεταβιβαζόμενες πληροφορίες ευαίσθητες σε πολλές κυβερνοεπιθέσεις. Πέρα των οικονομικών επιδιώξεων ή πρόκλησης βλαβών είτε σε άτομα (πχ δημοσίευση δεδομένων) είτε σε συσκευές, οι κακόβουλοι μπορούν να βλάψουν και την σωματική ακεραιότητα ατόμων, αφού το IoT βρίσκει εφαρμογή πλέον και στον τομέα της υγείας. Η διατήρηση της ασφάλειας πληροφοριών στα κοινόχρηστα δεδομένα που διακινούνται στο διαδίκτυο είναι ένα ιδιαίτερα σημαντικό ζήτημα [32]. (Pate, και συν., 2016)

Ευπάθειες και κενά ασφαλείας των συσκευών IoT καθιστούν τις επιθέσεις από Κυβερνοεγκληματίες, απλές και εύχρηστες. Στρατηγική πολλών επιθέσεων είναι η τοποθέτηση μίας συσκευής στο δίκτυο IoT και η εκτέλεση δόλιων πράξεων προς ένα άλλο συνδεδεμένο αντικείμενο, πλαστοπροσωπώντας το πραγματικό. Στα δίκτυα IoT κοινές επιθέσεις αποτελούν DoS, DDoS, routing attack, man in the middle, side channel attack, replay attack, node capture και mass node authentication.

Μια μελέτη του 2014 από την Hewlett-Packard σχετικά με εφαρμογές του Διαδικτύου των Πραγμάτων, αποκάλυψε ότι το 80% των συσκευών του παραβιάζει το απόρρητο των προσωπικών πληροφοριών (ευαίσθητα προσωπικά δεδομένα που προσωποποιούν τους χρήστες), το 80% απέτυχε να απαιτήσει κωδικούς πρόσβασης

με κατάλληλο μήκος και επαρκεί πολυπλοκότητα, το 70% δεν κρυπτογράφησε τις επικοινωνίες και το 60% είχε ευπάθειες ασφαλείας στις διεπαφές χρήστη τους.

2.1 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IOT

Οι ελάχιστες απαιτήσεις ασφαλείας που οφείλει να πληροί το IoT, σχετίζονται με ορισμένες βασικές αρχές . Καθένα από τα επίπεδα του συστήματος δικτύου IoT οφείλει να πληροί αυτές τις βασικές αρχές προκειμένου να μπορεί να χαρακτηριστεί ασφαλές ως προς την χρήση του. Οι συγκεκριμένες αρχές σχετίζονται, ως επί το πλείστον με τα δεδομένα του διακινούνται ανάμεσα στις όλο ένα και περισσότερες διασυνδεδεμένες συσκευές. Η ευκολία διασύνδεσης «έξυπνων» συσκευών στα συστήματα IoT δημιουργεί θέματα ασφαλείας, καθώς και θέματα που μπορεί να «θίξουν» την ιδιωτικότητα [82]. (Genc, et al., 2015).

Διάφοροι παράγοντες πρέπει να ληφθούν υπόψη κατά τη σχεδίαση λύσης ασφαλείας για τις συσκευές IoT. Οι βασικές απαιτήσεις ασφαλείας στα IoT συστήματα είναι εν συντομία (αναλυτικότερα βλ. Παράρτημα Γ):

- Η εμπιστευτικότητα δεδομένων,
- Η ακεραιότητα δεδομένων,
- Η ιδιωτικότητα δεδομένων,
- Η διαθεσιμότητα,
- Η ανθεκτικότητα και ευστάθεια,
- Η αξιοπιστία,
- Και ο έλεγχος πρόσβασης, έλεγχος ταυτότητας και εξουσιοδότηση.

2.2 ΠΕΡΙΟΡΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ ΣΤΟ IOT

Οι συσκευές στο IoT έχουν της τάση να συρρικνώνονται και να μειώνουν συνεχώς το κόστος τους. Οι περισσότερες συσκευές του, δεν έχουν σχεδιαστεί με γνώμονα την ασφάλεια. Κατά συνέπεια, έχουν προκύψει προβλήματα που σχετίζονται με δεδομένα που ανταλλάσσονται μεταξύ των δικτυωμένων συσκευών. Οι συσκευές του IoT είναι εγγενώς περιορισμένες σε πόρους σε αντίθεση με «παραδοσιακές» συσκευές. Η χρήση στο IoT συμβατικών μηχανισμών ασφαλείας που είναι ευρέως γνωστοί και αποδοτικοί και χρησιμοποιούνται στις «παραδοσιακές» συσκευές, είναι δύσκολη. Αυτό οφείλεται σε ιδιαίτερα χαρακτηριστικά που παρατηρούνται στις συσκευές του διαδικτύου των πραγμάτων. Τα ιδιαίτερα χαρακτηριστικά που διαφοροποιούν τις συσκευές IoT από τις παραδοσιακές συσκευές και δημιουργούν περιορισμούς ασφαλείας αφορούν στο υλικό, το λογισμικό και τα δίκτυα.

2.2.1 Περιορισμοί βάσει υλικού

Οι συσκευές στο IoT σε αντίθεση με «παραδοσιακές» συσκευές, σε επίπεδο hardware (υλικού) εμφανίζουν διαφοροποιήσεις. Το υλικό των συσκευών του IoT χαρακτηρίζεται από περιορισμένη μνήμη RAM και Flash. Λειτουργικά, χρησιμοποιούν κυρίως Real Time Operating System (RTOS) ή ελαφριά έκδοση του General Purpose Operating System (GPOS). Τα προηγμένα συστήματα ασφάλειας που χρησιμοποιούν τα παραδοσιακά ψηφιακά συστήματα απαιτούν υψηλή απόδοση όσον αφορά στη μνήμη. Η υψηλή απόδοση σε μνήμη που επιτυγχάνεται μέσω μεγάλης μνήμης RAM και σκληρών δίσκων επιτρέπει την ύπαρξη προηγμένων συστημάτων ασφάλειας (συμβατικοί αλγόριθμοι ασφαλείας) και έτσι, επιτυγχάνει υψηλό επίπεδο ασφαλείας. Ο περιορισμός στην μνήμη που εμφανίζουν οι συσκευές στο Διαδίκτυο των Πραγμάτων, δεν επιτρέπει ευθέως την υποστήριξη των συμβατικών αλγορίθμων ασφάλειας [71]. (RIOT: An Open Source Operating System for Low-end Embedded Devices in the IoT, 2018).

Επιπρόσθετα, ως προς το hardware των συσκευών του IoT, υπάρχει ενεργειακός και υπολογιστικός περιορισμός. Στο παραδοσιακό ψηφιακό σύστημα χρησιμοποιούνται κεντρικές μονάδες επεξεργασίας (CPU) υψηλής ισχύος με υψηλό ρυθμό ρολογιού, για την εξυπηρέτηση των αναγκών των συστημάτων. Τα παραπάνω συστήματα χαρακτηρίζονται από υψηλή κατανάλωση ενέργειας στα πλαίσια της λειτουργίας τους. Οι συσκευές στο IoT από την φάση σχεδιασμού τους, επιδιώκουν χαμηλές απαιτήσεις σε ισχύ σε συνδυασμό με όσο το δυνατόν χαμηλότερη κατανάλωση ενέργειας. Σε αντίθεση με τις παραδοσιακές συσκευές, χρησιμοποιούν CPU χαμηλής ισχύος με χαμηλό ρυθμό ρολογιού. Οι υπολογιστικοί και ενεργειακοί περιορισμοί δεν επιτρέπουν ευθέως την εγκατάσταση κρυπτογραφικών αλγορίθμων, οι οποίοι απαιτούν γρήγορους υπολογισμούς και μεγάλη επεξεργαστική ισχύ. Η χρήση των παραπάνω αλγορίθμων στα παραδοσιακά ψηφιακά συστήματα (π.χ. υπολογιστή) έχει θετική συνεισφορά στην ασφάλεια.

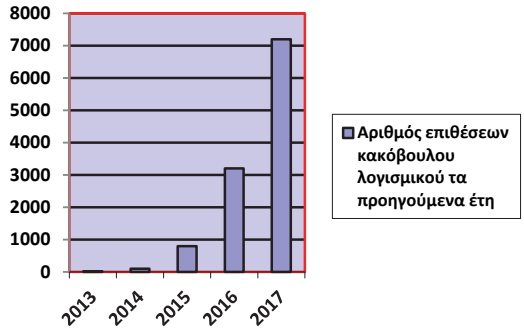
Εν κατακλείδι, η ευκολία της σύνδεσης των συσκευών στο IoT έχει καταστήσει δυσεπίτευκτο τον έλεγχο των συσκευών που συνδέονται. Αυτό δίνει «πρόσφορο έδαφος» σε κακόβουλους χρήστες, οι οποίοι εκμεταλλευόμενοι αυτό το γεγονός μπορούν να εξαγάγουν τα κρυπτογραφικά μυστικά, να τροποποιήσουν προγράμματα ή να τα αντικαταστήσουν με κακόβουλους κόμβους. Ενδεικτικά, η συσκευασία ανθεκτική σε παραβίαση μπορεί να αποτρέψει τέτοιες επιθέσεις κακόβουλων. Η συσκευασία ανθεκτική σε παραβίαση αναφέρεται, ουσιαστικά, στην «θωράκιση» του υλικού των συσκευών από επεμβατικές ή ημι-επεμβατικές επιθέσεις.

2.2.2 Περιορισμοί βάσει λογισμικού

Οι συσκευές στο IoT λόγω της αδύναμης επεξεργαστικής τους φύσης δεν δέχονται με ευκολία αναβαθμίσεις και ενημερώσεις έκδοσης κώδικα λογισμικού. Η δυσκολία εγκατάστασης μιας δυναμικής ενημερωμένης έκδοσης κώδικα ασφαλείας έχει ως αντίκτυπο να καθίσταται εξαιρετικά δύσκολη η εξάλειψη ή ο μετριασμός πιθανών τρωτών σημείων. Οι συσκευές του IoT σχεδιάστηκαν με λειτουργικό σύστημα ή στοίβα πρωτοκόλλου που στις περισσότερες περιπτώσεις ενδέχεται να μην

υπάρχει η δυνατότητα ενσωμάτωσης νέου κώδικα, βιβλιοθήκης ή ενημέρωσης του ήδη υπάρχοντος λογισμικού.

Επιπρόσθετα, το ενσωματωμένο λειτουργικό σύστημα των συσκευών του Διαδικτύου των Πραγμάτων χαρακτηρίζεται από λεπτές στοίβες πρωτοκόλλου δικτύου σε σχέση με τις παραδοσιακές συσκευές, στις οποίες υπάρχει στοίβα πρωτοκόλλου «χοντρή» με πλήθος λειτουργικών μονάδων ασφαλείας. Το παραπάνω χαρακτηριστικό των παραδοσιακών ψηφιακών συσκευών μετατρέπει την στοίβα πρωτοκόλλου τους ανεκτική σε σφάλματα που μπορεί να περιορίσουν την ασφάλεια τους. Στις συσκευές IoT, λόγω της ισχύος τους, η μονάδα ασφαλείας που έχει σχεδιαστεί για τη στοίβα πρωτοκόλλου πρέπει να είναι λεπτή. Ο παραπάνω περιορισμός δυσκολεύει τον σχεδιασμό μίας υψηλά ανθεκτικής μονάδας ασφαλείας με αποτέλεσμα σφάλματα να μπορούν να βλάψουν το λειτουργικό σύστημα και κατ' επέκταση ολόκληρη την υποδομή του IoT.



Γράφημα 1: Αριθμός επιθέσεων κακόβουλου λογισμικού στα συστήματα IoT τα προηγούμενα έτη.

2.2.3 Περιορισμοί βάσει δικτύων

Βασικά χαρακτηριστικά του IoT συναποτελούν η ετερογένεια, η συνδεσιμότητα, κλίμακα κ.α. Οι βασικές διαφορές των συσκευών του IoT σε σχέση με παραδοσιακές συσκευές σε επίπεδο δικτύου σχετίζονται με την φορητότητα που χαρακτηρίζει τις συσκευές IoT, καθώς και με την ποικιλομορφία στο δίκτυο που παρουσιάζουν οι συσκευές. Σαφή περιορισμό στο σχεδιασμό ενός ασφαλούς συστήματος IoT συντελεί η επεκτασιμότητα. Η ραγδαία αύξηση των διασυνδεδεμένων συσκευών στο δίκτυο πληροφοριών, καθημερινά περιορίζει τα

υπάρχοντα συστήματα ασφαλείας, τα οποία υστερούν όσον αφορά στην κλιμάκωση. Ως εκ τούτου, η έλλειψη της ιδιότητας της κλιμάκωσης των συστημάτων ασφαλείας των παραδοσιακών ψηφιακών συστημάτων δεν ενδείκνυται για τις IoT συσκευές.

Άλλη μία διαφοροποίηση που παρουσιάζουν οι συσκευές του IoT, είναι η κινητικότητα. Οι αλγόριθμοι που είχαν αναπτυχθεί στα πλαίσια της ασφάλειας παραδοσιακών συσκευών δεν είναι κατάλληλοι για τις συσκευές του IoT που παρουσιάζουν φορητότητα. Για την «θωράκιση» των IoT συσκευών, οι αλγόριθμοι ασφαλείας πρέπει να παρουσιάζουν ανθεκτικότητα στην κινητικότητα.

Η σύνδεση συσκευών στο IoT περιλαμβάνει ενσύρματες και ασύρματες ζεύξεις. Συσκευές συνεχώς, συνδέονται και αποσυνδέονται σε ένα δίκτυο IoT. Το παραδοσιακό μοντέλο ασφαλείας για τα παραδοσιακά ψηφιακά συστήματα δεν αντιμετωπίζει αυτού του είδους, τις ξαφνικές τοπικές αλλαγές δικτύου. Η δυναμική τοπολογία δικτύου απαιτεί ένα μοντέλο ασφαλείας με την δυνατότητα αντιμετώπισης αυτού του είδους την ιδιομορφία.

Παραδοσιακά, συσκευές σε ένα δίκτυο υπολογιστών χρησιμοποιούν το Internet Protocol standard (IP) για την επικοινωνία μεταξύ τους. Οι συσκευές στο Διαδίκτυο των Πραγμάτων επικοινωνούν με πολλαπλά πρωτόκολλα επικοινωνίας σε αντίθεση με τις παραδοσιακές συσκευές. Για παράδειγμα, σε ένα δίκτυο συσκευών IoT μπορεί να χρησιμοποιείται ένα ιδιόκτητο πρωτόκολλο δικτύου για την επικοινωνία μεταξύ των συσκευών και παράλληλα να επικοινωνεί με έναν πάροχο υπηρεσιών με το γνωστό IP πρωτόκολλο. Έτσι παραδοσιακοί μηχανισμοί ασφαλείας που ενδείκνυνται για την δικτύωση μονού πρωτοκόλλου είναι ανεπαρκείς για πολλαπλά πρωτόκολλα. Επίσης, οι συσκευές του IoT στο δίκτυο χαρακτηρίζονται από ποικιλομορφία. Ενδέχεται να είναι από απλές και γνωστές συσκευές, όπως για παράδειγμα ένας φορητός υπολογιστής μέχρι και πιο ιδιόμορφες συσκευές και συσκευές χαμηλού επιπέδου, όπως για παράδειγμα αισθητήρες και RFID tags. Παραδοσιακά, δεν υπήρχε μεγάλη ποικιλομορφία με αποτέλεσμα η εγκαθίδρυση μηχανισμού ασφαλείας να μην ήταν σύνθετη. Η ποικιλομορφία στα συστήματα IoT αποτελεί βασικό περιορισμό ως προς την χρήση συμβατικών μηχανισμών ασφαλείας.

2.3 ΚΙΝΔΥΝΟΙ ΣΤΟ IOT

Η ραγδαία εξάπλωση του IoT και η ένταξη του στην ανθρωπότητα σε συνδυασμό με την συνδεσιμότητα όλο και περισσότερων συσκευών στο IoT, συνεπάγεται την αύξηση των προσωπικών δεδομένων που διακινούνται. Οι μεταβιβαζόμενες πληροφορίες στα συστήματα IoT αποτελούν «στόχο» τρίτων. Το IoT δίνει χώρο σε πληθώρα κακόβουλων επιθέσεων. Στα συστήματα IoT έχουν δημιουργηθεί κενά ασφαλείας αφού η ιλιγγιώδη ταχύτητα αύξησης συνδέσεων συσκευών καθιστά των έλεγχο τους αδύνατο. Σε αντίθεση με τις παραδοσιακές συσκευές, στις συσκευές του IoT δίνεται έμφαση στην μείωση του κόστους και την συρρίκνωση των συσκευών. Αυτό το γεγονός, έχει ως αποτέλεσμα την έλλειψη της απαραίτητης επεξεργαστικής ισχύος. Η πλειοψηφία των συσκευών που λαμβάνουν τόπο στο IoT, δεν κατέχουν την απαραίτητη υπολογιστική ισχύ ή το κατάλληλο λογισμικό, ώστε να πραγματοποιήσουν πολύπλοκους υπολογισμούς για ασφαλή επικοινωνία ή η κρυπτογράφηση δεδομένων. Λόγω των περιορισμένων πόρων των συσκευών IoT, μηχανισμοί ασφαλείας, όπως το IDS ή το antivirus που διακρίνονται από αρκετή υπολογιστική ισχύ, δεν ενδείκνυνται για το IoT με αποτέλεσμα το λογισμικό να παρουσιάζει ευαισθησία. Η απώλεια της κρυπτογράφησης των δεδομένων στοιχίζει, όσον αφορά στα βασικά ζητήματα ασφαλείας, δηλαδή της εμπιστευτικότητα, της ακεραιότητας και της διαθεσιμότητας. Σε «παραδοσιακές» συσκευές που είναι συνδεδεμένες στο διαδίκτυο, χρησιμοποιείται συνδυασμός σουιτών ασφαλείας, οι οποίες εξασφαλίζουν σε υψηλό βαθμό την ιδιωτικότητα των δεδομένων. Παράδειγμα τέτοιας παραδοσιακής ψηφιακής συσκευής είναι ένας σταθερός ηλεκτρονικός υπολογιστής, ο οποίος έχει τεράστια υπολογιστική ικανότητα. Στις περισσότερες συσκευές του IoT τα λογισμικά του δεν χαρακτηρίζονται από ασφάλεια. Το λογισμικό των συσκευών δεν δέχεται ενημερώσεις, γεγονός που το καθιστά ευάλωτο σε επιθέσεις εφόσον ο κακόβουλος εντοπίσει ευπάθεια σε αυτό.

Πρόβλημα των συστημάτων IoT ως προς την ασφάλεια, αποτελεί ο έλεγχος ταυτότητας των πραγμάτων και η εξουσιοδότηση. Ερευνητές προσπαθούν να επιλύσουν το πρόβλημα της πιστοποίησης αντικειμένων και της εξουσιοδότησης αλλά συντελεί πολύ δύσκολο ζήτημα προς επίλυση. Στις «παραδοσιακές» συσκευές το πρόβλημα επιλυόταν με πολλές μεθόδους, όπως τον κωδικό πρόσβασης, τα προ-

κοινόχρηστα μυστικά και κρυπτό-συστήματα δημόσιου κλειδιού. Οι παραδοσιακοί μέθοδοι ελέγχου ταυτότητας και εξουσιοδότησης στα αντικείμενα του IoT δεν μπορούν να εφαρμοστούν λόγω της ετερογένειας που αποτελεί βασικό χαρακτηριστικό τους και της πολυπλοκότητας των αντικειμένων και των δικτύων (διαφορετικά πρωτόκολλα επικοινωνίας). Η επεκτασιμότητα ως προς το συνεχώς αυξανόμενο πλήθος των διασυνδεδεμένων συσκευών καθιστά την διαχείριση των κλειδιών ένα πολύ δύσκολο ζήτημα. Επιπρόσθετα, τα διαπιστευτήρια που χρησιμοποιούνται στα συστήματα IoT είναι αδύναμα με αποτέλεσμα να δημιουργούν ανασφαλή διαδικτυακή επαφή. Με την ραγδαία εξάπλωση του IoT, πολλοί ερευνητές «έθιξαν» το θέμα της ιδιωτικότητας και του απορρήτου των προσωπικών δεδομένων. Οι πληροφορίες και τα δεδομένα με την χρήση του IoT, δεν περιορίζονται μόνο στην σχετική συμπεριφορά στο διαδίκτυο, αλλά και στην καθημερινότητα του χρήστη. Οι πληροφορίες και τα δεδομένα αφορούν, πλέον, σε ευαίσθητα προσωπικά δεδομένα, διότι περιγράφουν λεπτομερώς τον χρήστη (το υποκείμενο των δεδομένων). Αποτέλεσμα της κακής χρήσης προσωπικών δεδομένων καθώς και κακόβουλων συμπεριφορών είναι να «θιχτεί» το βασικό ζήτημα της ιδιωτικότητας [31]. (Ullah, et al., 2017).

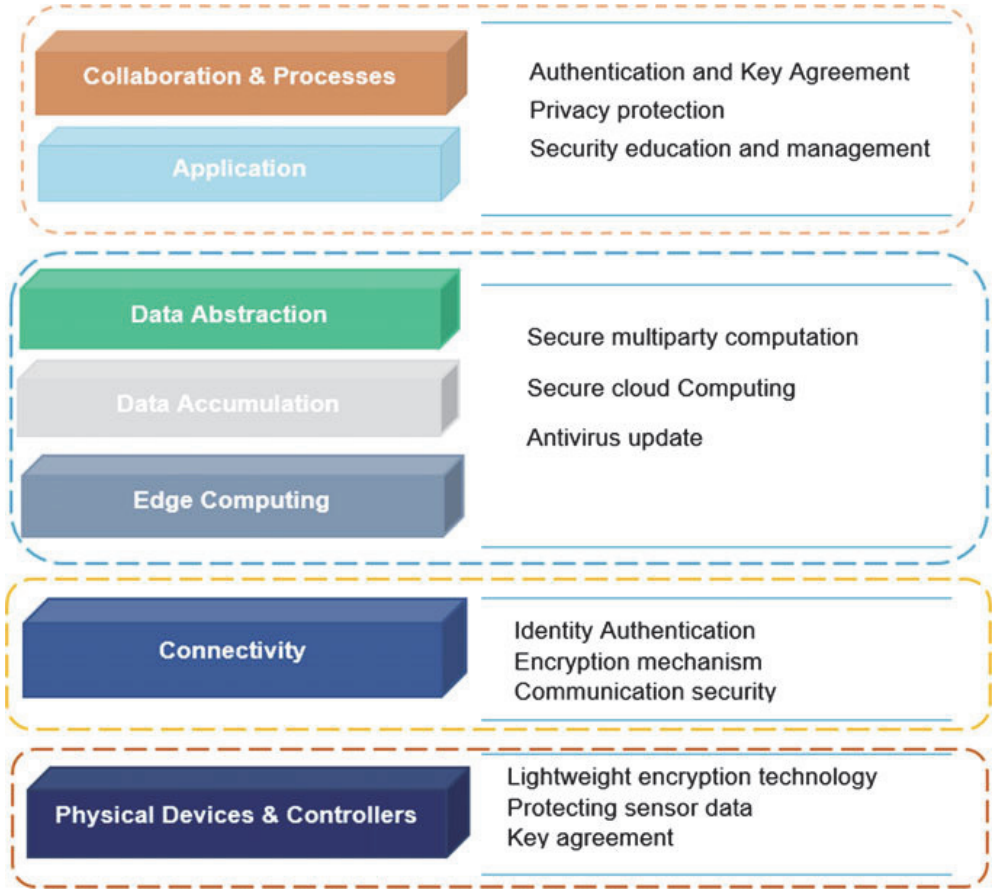
2.4 ΠΡΟΚΛΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΡΩΜΑΤΩΝ ΤΟΥ IOT

Τα στρώματα που σχετίζονται με την αρχιτεκτονική του IoT είναι το επίπεδο ανίχνευσης, το επίπεδο δικτύου και πυλών, το επίπεδο διαχείρισης υπηρεσίας και το

επίπεδο εφαρμογής. Στοιχεία ασφαλείας που σχετίζονται με κάθε στρώμα είναι η εξουσιοδότηση, ο έλεγχος πρόσβασης, ο έλεγχος ταυτότητας, η εμπιστευτικότητα δεδομένων, η διαθεσιμότητα δεδομένων, η ακεραιότητα δεδομένων, η ικανότητα αντιμετώπισης κακόβουλου λογισμικού και η ανθεκτικότητα απέναντι σε επιθέσεις. Οι συσκευές του IoT λόγω διαφοροποιήσεων στο υλικό συγκριτικά με παραδοσιακές συσκευές, όπως αναλύθηκαν παραπάνω, δεν θωρακίζονται από συμβατούς μηχανισμούς ασφαλείας. Κάθε στρώμα είναι ευαίσθητο σε απειλές και επιθέσεις που υποβαθμίζουν την ασφαλεία [34]. (Atlam, et al., 2018).

Οι απειλές συντελούν «προϊόν» κακόβουλων δραστηριοτήτων, οι οποίες πραγματοποιούνται από τρίτα πρόσωπα που στοχεύουν στην πρόκληση ζημιών. Οι προαναφερθέντες απειλές, προκαλούνται από επιθέσεις κυβερνο-εγκληματιών, οι οποίοι χαρακτηρίζονται από καλές δεξιότητες και ικανότητες και έχουν στην διάθεση τους προηγμένο εξοπλισμό και λογισμικό. Οι διαφορές που παρουσιάζονται στις συσκευές του IoT σε σχέση με τις παραδοσιακές συσκευές δημιουργούν ευπάθειες.

Οι επιθέσεις που λαμβάνουν χώρα στο IoT ανάλογα με το είδος τους, μπορεί να διακριθούν σε ενεργές επιθέσεις και σε παθητικές επιθέσεις. Οι τελευταίες σχετίζονται με την δυνατότητα παρακολούθησης των δεδομένων και των πληροφοριών στο δίκτυο IoT. Επιπλέον, έχουν το χαρακτηριστικό ότι δεν γίνονται άμεσα αντιληπτές, επειδή δεν παρεμποδίζουν τις υπηρεσίες του IoT. Αντιθέτως, οι ενεργές επιθέσεις γίνονται εύκολα αντιληπτές, αφού παρεμποδίζουν την υπηρεσία. Για την εγκαθίδρυση ασφάλειας στο IoT απαιτείται κάθε στρώμα να παρέχει αμυντικούς μηχανισμούς (βλ. Παράρτημα Γ) και να μην υπάρχουν τρωτά σημεία [31]. (Ullah, et al., 2017).



Εικόνα 5: Απαιτήσεις ασφαλείας σε κάθε επίπεδο της αρχιτεκτονικής του IoT[7] [81]. (Atlam, και συν., 2019)

2.4.1 Θέματα ασφάλειας στο στρώμα Ανίχνευσης

Το επίπεδο ανίχνευσης, όπως αναλύθηκε στο πρώτο κεφάλαιο, αποτελεί το χαμηλότερο επίπεδο και περιλαμβάνει συσκευές ανίχνευσης, ασύρματα δίκτυα αισθητήρων, ενεργοποιητές, ελεγκτές, και ετικέτες ραδιοσυχνοτήτων RFID. Οι συσκευές αυτές οφείλουν να είναι σε θέση να αποδείξουν την ταυτότητά τους και να παρέχουν δεδομένα αναλλοίωτα σε συνεχή ροή, ώστε να χαρακτηρίζονται από τις βασικές αρχές της ακεραιότητας και της διαθεσιμότητας και να περιορίσουν ως προς στην ορατότητα και την πρόσβαση τα τοπικά αποθηκευμένα δεδομένα για την

[7] https://www.researchgate.net/figure/Security-requirements-at-each-level-of-the-IoT-architecture_fig1_332859761

εξασφάλιση της εμπιστευτικότητας. Το στρώμα ανίχνευσης του IoT απαρτίζεται κυρίως από αισθητήρες και RFID, των οποίων ο αποθηκευτικός χώρος, η κατανάλωση ισχύος και η υπολογιστική ικανότητα είναι περιορισμένες σε σχέση με τα παραδοσιακά ψηφιακά συστήματα. Τα παραπάνω χαρακτηριστικά προϊκονομούν την αδυναμία υποστήριξης συμβατών μηχανισμών ασφαλείας.

Σε αυτό το επίπεδο, προέκυψαν τρία ζητήματα που θέτουν σε κίνδυνο το IoT. Οι συσκευές του IoT σε αντίθεση με τις παραδοσιακές συσκευές επικοινωνούν μέσω ασύρματων σημάτων. Η μεταβίβαση των πληροφοριών από αισθητήρες γίνονται μέσω των παραπάνω σημάτων. Παρεμβολές στα ασύρματα σήματα μπορούν να αποβούν «μοιραίες» ως προς την την αξιοπιστία τους. Επιπλέον, οι κόμβοι στα IoT παρευρίσκονται συνήθως σε εξωτερικά περιβάλλοντα. Η τοπολογία των αισθητήρων, επιτρέπει την απειλή μέσω φυσικών επιθέσεων από κακόβουλους. Ο επιτιθέμενος παραβιάζοντας το υλικό μπορεί να προκαλέσει φθορές σε όλη την υποδομή του συστήματος IoT. Τέλος, σε αυτό το επίπεδο, κρίσιμο ζήτημα στα πλαίσια της ασφαλείας συντελεί η εγγενής φύση της τοπολογίας δικτύου. Τα συστήματα IoT χαρακτηρίζονται από δυναμική τοπολογία δικτύου, καθώς οι κόμβοι του IoT μετακινούνται συχνά σε διαφορετικά μέρη [31]. (Ullah, et al., 2017)

2.4.2 Θέματα ασφάλειας στο στρώμα Δικτύου

Το επίπεδο δικτύου αποτελεί το επίπεδο που δίνει πρόσβαση στο διαδίκτυο και είναι αρμόδιο για την συνδεσιμότητα, για την μετάδοση δεδομένων, καθώς και για την παροχή υπηρεσιών cloud. Οι περιορισμένοι πόροι και μνήμη που χαρακτηρίζουν τις συσκευές του IoT συγκριτικά με τα παραδοσιακά ψηφιακά συστήματα, περιορίζουν την χρήση των συμβατών διαδικασιών κρυπτογράφησης. Επιπρόσθετα, τα διαφορετικά πρωτόκολλα που χρησιμοποιούν οι συσκευές του IoT στα πλαίσια της επικοινωνίας αποτελούν έναν ιδιαίτερα σημαντικό περιορισμό. Στα συστήματα IoT, η επικοινωνία ανατίθεται στις πύλες, οι οποίες συμβάλλουν στη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και των δεδομένων. Οι πύλες περιλαμβάνουν υλικό και λογισμικό και έχουν την δυνατότητα επεξεργασίας μίας πληροφορίας και αξιοποίησής της.

Η επικοινωνία στο IoT είναι διαφορετική από αυτήν του Διαδικτύου, καθώς δεν περιορίζεται μόνο στα πλαίσια μηχανής και ανθρώπου. Αυτό το γεγονός, δημιουργεί θέματα συμβατότητας που σε παραδοσιακά συστήματα δεν παρουσιαζόταν. Τα πρωτόκολλα δικτύου παραδοσιακών συστημάτων δεν ενδείκνυνται για τα συστήματα IoT που παρουσιάζουν ετερογένεια. Η κλιματωσιμότητα των IoT και η συνεχή σύνδεση συσκευών δίνει πρόσφορο έδαφος σε επιτιθέμενους να αποκτήσουν τεράστιο όγκου δεδομένων που πολλές φορές μπορεί να αποτελούν και ευαίσθητα προσωπικά δεδομένα. Η προστασία, λοιπόν, αυτού του επιπέδου του IoT αποτελεί σημαντική προϋπόθεση για την θωράκιση του συστήματος.

Επιθέσεις που σχετίζονται με αυτό το στρώμα, μπορούν να διαταράξουν το απόρρητο και επομένως να αποτελέσουν πηγή διαρροής δεδομένων. Χαρακτηριστική επίθεση που σχετίζεται άμεσα με το στρώμα αυτό είναι η επίθεση «Man in the Middle». Καλά σχεδιασμένοι μηχανισμοί ανταλλαγής κλειδιών και υλικό κλειδώματος μπορούν να αποτρέψουν την πλήρη παραβίαση του καναλιού επικοινωνίας και κατ΄ επέκταση την κλοπή ταυτότητας των συσκευών [31]. (Ullah, et al., 2017)

2.4.3 Θέματα ασφάλειας στο στρώμα Υπηρεσιών

Το επίπεδο υπηρεσιών χαρακτηρίζεται για την διαχειριστική ικανότητα του πάνω στις οντότητες του IoT. Η διαχείριση αυτή επιτυγχάνεται με την χρήση αναλυτικών μεθόδων που πλαισιώνουν το επίπεδο αυτό. Λόγω της ραγδαίας σύνδεσης συσκευών στο IoT, ο έλεγχος τους αποτελεί πολύπλοκη και δύσκολη εργασία. Για την ασφάλεια των συστημάτων, σημαντικές κρίνονται οι διαδικασίες ελέγχου πρόσβασης, ελέγχου ταυτότητας και εξουσιοδότησης. Τα δεδομένα παρακολούθησης αποτελούν ένα σημαντικό αντίμετρο για κακόβουλες δραστηριότητες, καθώς μπορούν να ανιχνεύσουν μη φυσιολογικές συμπεριφορές.

Το στρώμα αυτό, παρουσιάζει ευαισθησία σε επιθέσεις άρνησης υπηρεσίας. Οι επιθέσεις άρνησης εξυπηρέτησης και κατανεμημένης-άρνησης εξυπηρέτησης λειτουργικά, καθιστούν τις συσκευές και τους πόρους μη διαθέσιμα σε εξουσιοδοτημένους χρήστες.

2.4.4 Θέματα ασφάλειας στο στρώμα Εφαρμογών

Στο στρώμα εφαρμογών περιλαμβάνονται οι πλατφόρμες IoT, οι οποίες ενεργοποιούν τις εφαρμογές IoT παρέχοντας μια γρήγορη απόκριση των υπηρεσιών του. Το επίπεδο αυτό υποστηρίζει όλα τα είδη επιχειρηματικών λειτουργιών, κάνει έξυπνους υπολογισμούς και έχει την δυνατότητα επεξεργασίας δεδομένων. Τα δεδομένα που καλείται να διαχειριστεί χαρακτηρίζονται από τεράστιο όγκο. Στις παραδοσιακές συσκευές ο αποθηκευτικός χώρος είναι επαρκής για την υποστήριξη του μεγάλου πλήθους δεδομένων. Οι συσκευές στο IoT δεν περιλαμβάνουν μεγάλους αποθηκευτικούς χώρους. Ο περιορισμός της μνήμης σε συνδυασμό με τον τεράστιο αριθμό συνδεδεμένων συσκευών που μοιράζονται πληροφορίες θα προκαλέσουν μεγάλη επιβάρυνση σε εφαρμογές που αναλύουν τα δεδομένα, αποτελώντας ζήτημα και πρόκληση ως προς την διαθεσιμότητα των υπηρεσιών.

Το επίπεδο αυτό, χαρακτηρίζεται από πλήθος διαφορετικών εφαρμογών. Η ποικιλομορφία και το πλήθος τους περιλαμβάνει διαφορετικούς μηχανισμούς ελέγχου ταυτότητας. Η ενσωμάτωση όλων των ελέγχων ταυτότητας αποτελεί μία πολύ δύσκολη εργασία με αποτέλεσμα η διασφάλιση της ιδιωτικής ζωής των δεδομένων να αποτελεί δύσκολο έργο [31].

2.5 ΕΠΙΘΕΣΕΙΣ ΣΕ ΣΥΣΤΗΜΑΤΑ IOT

Το IoT εξαπλώνεται με ταχύ ρυθμό και ενσωματώνεται σε όλο και περισσότερες κοινωνικές δομές γεγονός που επιθέσεις στον κυβερνοχώρο δεν είναι απλώς εικονικές αλλά έχουν και φυσική υπόσταση. Τα ειδικά χαρακτηριστικά των συσκευών IoT, όπως το χαμηλό κόστος τους, η χαμηλή ισχύ και υπολογιστική ικανότητα, η ετερογένεια και η μεγάλη κλίμακα του δικτύου περιορίζουν την εφαρμογή συμβατικών μηχανισμών ασφαλείας που χρησιμοποιούνταν σε παραδοσιακά ψηφιακά συστήματα. Επομένως, τα συστήματα IoT είναι επιρρεπή σε πολλές προηγμένες επιθέσεις που απαιτούν νέους και πιο σύνθετους μηχανισμούς ασφαλείας βάση των «ειδικών» χαρακτηριστικών τους. Παραδείγματα μηχανισμών ασφαλείας αποτελούν η αναγνώριση/έλεγχος ταυτότητας που αποβλέπουν στην

αξιοπιστία, στην εμπιστευτικότητα και στην ανθεκτικότητα των δεδομένων που χρησιμοποιούν και επεξεργάζονται συστήματα[60]. (Chen, et al., 2011)

Ο όρος «επίθεση» στα πλαίσια του IoT αναφέρεται σε οποιαδήποτε κακόβουλη ενέργεια που πραγματοποιείται μέσω λογισμικού, δικτύου και υλικού και έχει στόχο την τροποποίηση δεδομένων, την ολική καταστροφή πληροφοριών, την υποκλοπή δεδομένων, την διαρροή τους ή την μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και πληροφορίες του νόμιμου κατόχου τους. Οι ευπάθειες που παρουσιάζουν τα συστήματα του Διαδικτύου των Πραγμάτων καθιστούν τις επιθέσεις σε αυτό πιο εύκολες και εύχρηστες.

Σε άρθρο στο Forbes το 2014, αναφέρεται πλήθος καθημερινών δικτυωμένων συσκευών, οι οποίες εκτελούν ετερογενείς δραστηριότητες που βρίσκονται στα ετερογενή δίκτυα και επικοινωνούν μεταξύ τους μέσω ετερογενών πρωτοκόλλων επικοινωνίας. Στα πλαίσια του IoT οι δικτυωμένες συσκευές μπορούν να αποτελέσουν «πηγή κατασκοπείας του ανθρώπου μέσα στο ίδιο του το σπίτι».

Οι επιθέσεις στο IoT ανάλογα με την συμπεριφορά τους μπορούν να κατηγοριοποιηθούν σε τέσσερα επίπεδα. Εν’ συντομία οι επιθέσεις διακρίνονται σε (Ullah, et al., 2017):

- Επίθεση χαμηλού επιπέδου: Το επίπεδο αυτό αφορά ανεπιτυχείς επιθέσεις. Ο κακόβουλος κατορθώνει να επιτεθεί στο δίκτυο του IoT, χωρίς αποτέλεσμα.
- Επίθεση μεσαίου επιπέδου: Το επίπεδο αυτό αφορά επιθέσεις κατασκοπίας. Ο κακόβουλος χρήστης εισβάλει στο σύστημα και αποκτά πρόσβαση σε δεδομένα και πληροφορίες. Σε αυτού του επίπεδου τις επιθέσεις δεν διακινδυνεύεται η ακεραιότητα δεδομένων και πληροφοριών, αφού ο εισβολέας αδυνατεί να τροποποιήσει ή ακόμα και να προκαλέσει ολική καταστροφή των δεδομένων.
- Επίθεση υψηλού επιπέδου: Οι επιθέσεις υψηλού επιπέδου πέρα της κατασκοπείας μεταβάλλουν τα δεδομένα και τις πληροφορίες. Το επίπεδο αυτό περιλαμβάνει επιθέσεις που τροποποιούν ή ακόμα και καταστρέφουν πληροφορίες και δεδομένα με αποτέλεσμα να θίγουν το ζήτημα της ακεραιότητας τους.

- Επίθεση εξαιρετικά υψηλού επιπέδου: Πραγματοποιώντας τέτοιου επιπέδου επιθέσεις σε δίκτυο, ο κακόβουλος χρήστης αποκτά μη εξουσιοδοτημένη πρόσβαση. Ο εισβολέας εκτελεί παράνομες δραστηριότητες προκαλώντας παρεμβολές στο δίκτυο και καθιστώντας το μη διαθέσιμο.

Διάφοροι τύποι επιθέσεων εκμεταλλεύονται ευπάθειες του IoT που σε πολλές περιπτώσεις έχουν τεράστιο αντίκτυπο. Ως προς το τύπο των επιθέσεων διακρίνονται σε επιθέσεις πλαστοποίησης πληροφοριών, σε επιθέσεις επανάληψης πληροφοριών δρομολόγησης, σε επιθέσεις με βάση το επίπεδο πρόσβασης, σε επιθέσεις σε πρωτόκολλα επικοινωνίας, σε επιθέσεις με βάση την ιδιότητα της συσκευής, σε επιθέσεις με βάση τη μετάδοση δεδομένων και επιθέσεις με κεντρικό υπολογιστή. Ευρέως διαδεδομένες επιθέσεις σε συστήματα IoT είναι οι spoofing, replay routing attack, DDoS, DoS, timming attack, node capture attack και Sybil attack.

Γνωστές επιθέσεις, όπως timming attack, spoofing, replay routing και node capture αποτελούν απειλές που συγκαταλέγονται στον τύπο πλαστοποίησης πληροφοριών δρομολόγησης, αλλαγή ή επανάληψη πληροφοριών δρομολόγησης. Ο εισβολέας μπορεί με αυτό το τύπο επιθέσεων να «θίξει» βασικά ζητήματα ασφαλείας, συγκεκριμένα την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Οι επιθέσεις αυτού του τύπου απειλούν τα συστήματα IoT, αφού μέσω αυτών ο κακόβουλος μπορεί να μεταβάλει τις πληροφορίες δρομολόγησης πακέτων στα πλαίσια επικοινωνίας πετυχαίνοντας το, μέσω πλαστοποίησης της ταυτότητας του πραγματικού πομπού. Οι επιθέσεις αυτές δίνουν την δυνατότητα σε κυβερνο-εγκληματίες να λαμβάνουν τα δεδομένα και να απόστέλλουν κακόβουλες πληροφορίες στο δίκτυο IoT εισάγοντας κόμβο στο σύστημα. Κατα αυτό το γεγονός απειλούν το ζήτημα της εμπιστευτικότητας των πληροφοριών που μεταβιβάζονται.

Η κατηγορία των επιθέσεων με βάση το επίπεδο πρόσβασης, σχετίζεται με τις ενεργητικές και παθητικές επιθέσεις. Αναλυτικότερα, οι παθητικές επιθέσεις αποτελούν οι επιθέσεις κατασκοπείας. Αυτές οι απειλές βλάπτουν την βασική απαίτηση της εμπιστευτικότητας. Οι ενεργές επιθέσεις αφορούν το σύνολο των επιθέσεων που τείνουν να βλάψουν την συνδεσιμότητα και την επικοινωνία, η οποία αποτελεί βασικό χαρακτηριστικό των IoT συστημάτων. Επιπρόσθετα, οι παραπάνω επιθέσεις μπορούν να τροποποιήσουν τις πληροφορίες δρομολόγησης των πακέτων

με αποτέλεσμα, δεδομένα και πληροφορίες να μην «φτάνουν» ποτέ στον νόμιμο δέκτη.

Στην επικοινωνία των συνδεδεμένων οντοτήτων στα πλαίσια του IoT παρουσιάζεται ποικιλομορφία αναλογικά με τα πρωτόκολλα επικοινωνίας σε αντίθεση με τα παραδοσιακά συστήματα που χρησιμοποιείται μόνο το πρωτόκολλο TCP/IP. Οι λειτουργίες επικοινωνίας των δικτύων IoT αφορούν, στο συνδυασμό πρωτοκόλλων, όπου άλλα πρωτόκολλα σε συνδυασμό με το TCP/IP περιγράφουν το δίκτυο στα πλαίσια της επικοινωνίας. Η διαφορετικότητα αυτή δημιουργεί τρωτότητα, αφού συμβατοί μηχανισμοί ασφαλείας δεν ενδείκνυνται για την κάλυψη της ασφάλειας του συστήματος. Οι εισβολείς εκμεταλλεύονται αυτή την ευπάθεια και επιτίθονται στα πρωτόκολλα επικοινωνίας.

Οι κακόβουλοι επίσης μπορεί να έχουν και φυσική εμπλοκή. Μπορούν να εκμεταλλευτούν την φυσική τοπολογία των συστημάτων IoT, η οποία χαρακτηρίζεται από απομακρυσμένες συσκευές που πολλές φορές βρίσκονται σε εξωτερικό περιβάλλον. Αυτό το χαρακτηριστικό αποτελεί φυσική «πόρτα» για τους εισβολείς οι οποίοι παραβιάζοντας το υλικό μπορούν να βλάψουν όλη την υποδομή του IoT και κατ' επέκταση τους χρήστες.

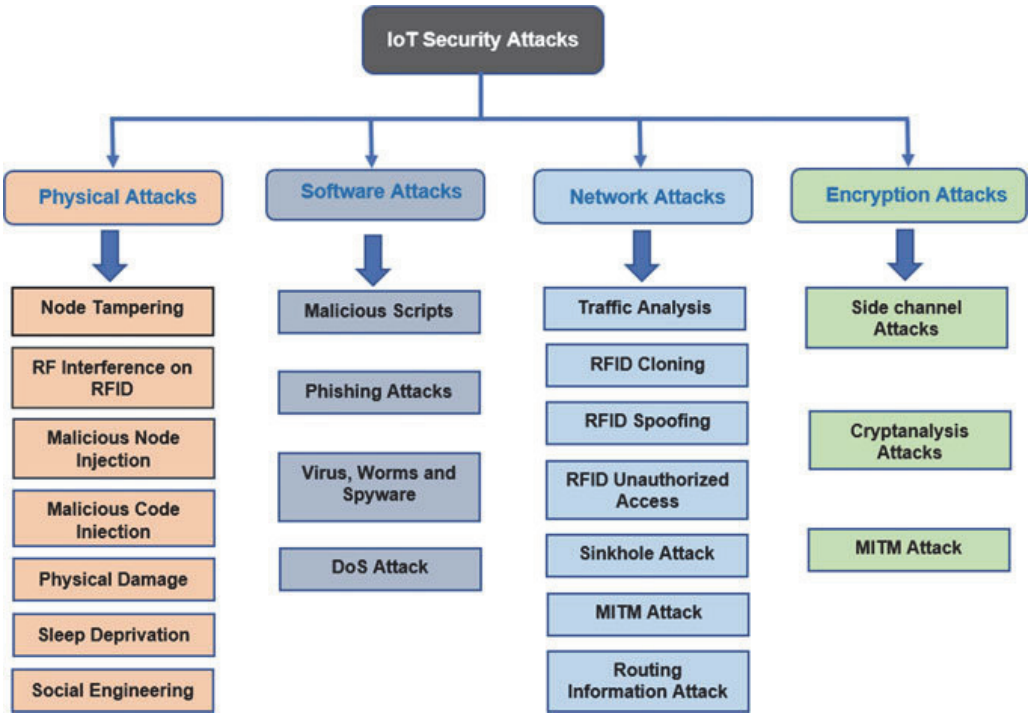
Πολλές επιθέσεις εκμεταλλεύονται τα χαρακτηριστικά και τις ιδιότητες των συνδεδεμένων συσκευών. Οι συσκευές του IoT ανάλογα με την ισχύ τους και την ενέργεια κατηγοριοποιούνται σε δύο ομάδες. Το IoT απαρτίζεται κυρίως από συσκευές χαμηλής κατανάλωσης ενέργειας και ισχύος. Οι επιθέσεις της κατηγορίας χαμηλού επιπέδου συσκευών εκμεταλλεύονται την έλλειψη κρυπτογράφησης στη τεχνολογία RFID των IoT. Ο κακόβουλος χρήστης μπορεί να συγκεντρώσει τα δεδομένα μίας ετικέτα, ή ακόμα και να κλωνοποιήσει την ετικέτα. Δημοφιλή επίθεση που εκμεταλλεύεται την κλωνοποιούμενη ετικέτα αποτελεί η skimming στην οποία ο εισβολέας αποκτά την ετικέτα του προϊόντος. Η κλωνοποίηση ετικετών επιτυγχάνεται και με αντίστροφη μηχανική κατά την οποία δίνεται η δυνατότητα στο επιτιθέμενο, αφού αποκτήσει την ετικέτα και κατ' επέκταση τον κωδικό, να χρησιμοποιήσει τον κλώνο για την αντικατάσταση της νόμιμης ετικέτας. Οι επιθέσεις κλάσης συσκευών υψηλού επιπέδου περιλαμβάνουν επιθέσεις σε συσκευές με ισχυρή υπολογιστική ισχύ και ενεργοβόρες. Σε αυτόν τον τύπο επιθέσεων συγκαταλέγονται επιθέσεις, όπου οι κακόβουλοι εκμεταλλεύονται και χρησιμοποιούν την υπολογιστική ισχύ των CPU και των GPU για να ξεκινήσουν παράνομες δραστηριότητες στο IoT δίκτυο. Τέτοιες

συσκευές με υψηλή ισχύ και ενέργεια συντελούν οι σταθεροί και φορητοί υπολογιστές.

Ευάλωτα σε επιθέσεις στο διαδίκτυο των πραγμάτων είναι επίσης και τα ασύρματα δίκτυα αισθητήρων (WSN), τα οποία αποτελούν τεχνολογία απαραίτητη για λειτουργικότητα του. Η επίθεση man in the middle εκμεταλλεύεται τον τρόπο μετάδοσης δεδομένων, αφού ένας κακόβουλος έχει την δυνατότητα να παρακολουθήσει την επικοινωνία και να διαταράξει την μετάδοση δεδομένων και πληροφοριών. Οι αισθητήρες είναι επιρρεπείς σε διάφορα είδη επιθέσεων που δίνουν την δυνατότητα σε εισβολείς να εκκινήσουν επιθέσεις στο επίπεδο δικτύου των IoT. Η τεχνολογία των αισθητήρων παρουσιάζει τρωτότητα, σε επιθέσεις που μπορούν να προκαλέσουν διακοπή, υποκλοπή πληροφοριών και αλλαγή/τροποποίηση.

Σημαντική κατηγορία επιθέσεων αποτελεί η κατηγορία που αφορά επιθέσεις με κεντρικό υπολογιστή. Στόχος των κακόβουλων είναι οι πόροι του κεντρικού υπολογιστή (π.χ. υλικό). Οι κακόβουλοι σε αυτή την κατηγορία επιθέσεων στοχεύουν τους πόρους των συσκευών του IoT γεγονός που μπορεί να επηρεάσει όλη την υποδομή του.

Με βάση τη γραμμή παραγωγής για ολοκληρωμένα κυκλώματα (IC), υπάρχουν πολλές ευπάθειες που βασίζονται στο σχεδιασμό του υλικού. Ορισμένες δημοφιλείς απειλές ως προς το υλικό αποτελούν το ψεύτικο αντίγραφο, η επίθεση πλευρικού καναλιού, η αντίστροφη μηχανική, η αεροπειρατεία πνευματικής ιδιοκτησίας (IP) και Trojan υλικού.



Εικόνα 6: Διάφορες επιθέσεις στα συστήματα IoT[8]. [81] (Atlam, και συν., 2019)

[8] https://www.researchgate.net/

2.6 ΕΠΙΘΕΣΕΙΣ ΣΤΟ ΥΛΙΚΟ ΤΩΝ ΣΥΣΚΕΥΩΝ

Οι επιθέσεις στο υλικό και στα ενσωματωμένα συστήματα αποτελούν αυξανόμενη ανησυχία καθώς ο αριθμός των συσκευών στα πλαίσια του IoT αυξάνεται εκθετικά. Τα αντίμετρα με χρήση λογισμικού σε επιθέσεις, δεν έχουν την δυνατότητα εξ' ολοκλήρου θωράκισης του συστήματος IoT, καθώς επιτιθέμενοι μπορούν να αποκτήσουν δεδομένα και πληροφορίες από «πόρτες» στα φυσικά μέσα. Δούρειοι Ίπποι στο υλικό, παραβίαση πνευματικής ιδιοκτησίας (IP), η μέθοδος της αντίστροφης μηχανικής, η επίθεση πλευρικού καναλιού και το ψεύτικο αντίγραφο συντελούν δημοφιλείς και κοινές επιθέσεις στο υλικό στα δίκτυα IoT.

Οι επιθέσεις στο φυσικό μέσο χωρίζονται σε τρεις κατηγορίες ανάλογα με τον τύπο τους. Οι μη επεμβατικές επιθέσεις που χαρακτηρίζονται από χαμηλό κόστος δεν προϋποθέτουν καμία γνώση από πλευράς επιτιθέμενου ώς προς την εσωτερική λειτουργία του «στόχου» και δεν περιλαμβάνουν καμία φυσική αλλοίωση. Οι επεμβατικές επιθέσεις από την άλλη, χαρακτηρίζονται από υψηλό κόστος και προϋποθέτουν την πλήρη γνώση της εσωτερικής λειτουργίας του «στόχου» και περιλαμβάνουν ιδιαίτερα σημαντική φυσική αλλοίωση του μέσου. Τέλος, οι ημι-επεμβατικές επιθέσεις που είναι ενδιάμεσου κόστους, προϋποθέτουν την μερική γνώση της εσωτερικής λειτουργίας του «στόχου» και η φυσική αλλοίωση του μέσου είναι ελάχιστη.

Άλλες επιθέσεις που σχετίζονται με το υλικό των συσκευών είναι επιθέσεις χρονισμού, επιθέσεις cache, εκπομπές ηλεκτρομαγνητικών πεδίων και επιθέσεις αλυσιδωτής σάρωσης. Οι επιτιθέμενοι μέσω αυτών των επιθέσεων εκμεταλλεύονται ευπάθειες που βασίζονται σε σχέδια υλικού. Το αντίκτυπο αυτών των επιθέσεων είναι σε πολλές περιπτώσεις τεράστιο, αφού ο κίνδυνος παραβιάσεων που μπορεί να οδηγήσουν σε απώλειες μεγάλων χρηματικών ποσών από κλεμμένα δεδομένα ή αντιγραμμένα IP. Η άμυνα σε αυτές τις επιθέσεις βασίζεται σε στοιχεία που διασφαλίζουν την ασφάλεια υλικού, την ασφάλεια σχεδιασμού και την ασφάλεια

δεδομένων [63]. (A survey on Internet of Things: Architecture, Enabling Technologies, Security andPrivacy, and Applications, 2017).

Η ραγδαία ανάπτυξη των συσκευών IoT σε συνδυασμό με την έλλειψη καθολικών κατασκευαστικών προτύπων και την υψηλή ζήτηση συσκευών χαμηλού κόστους, συνεπάγονται με την αναμονή εφαρμογής επιθέσεων υλικού σε συσκευές IoT από κακόβουλα άτομα. Η ανάπτυξη αυτή που παρουσιάζεται στα IoT συστήματα, εντείνει την ανησυχία αναφορικά με επιθέσεις που θα μπορούσαν να είχαν καταστροφικά αποτελέσματα. Οι PUF αποτελούν σημαντικό αντίμετρο σε επιθέσεις που σχετίζονται με το IoT, παρέχοντας ασφαλή αναγνώριση αντικειμένων και εξαλείφοντας ή μετριάζοντας κινδύνους από επιθέσεις τρίτων.

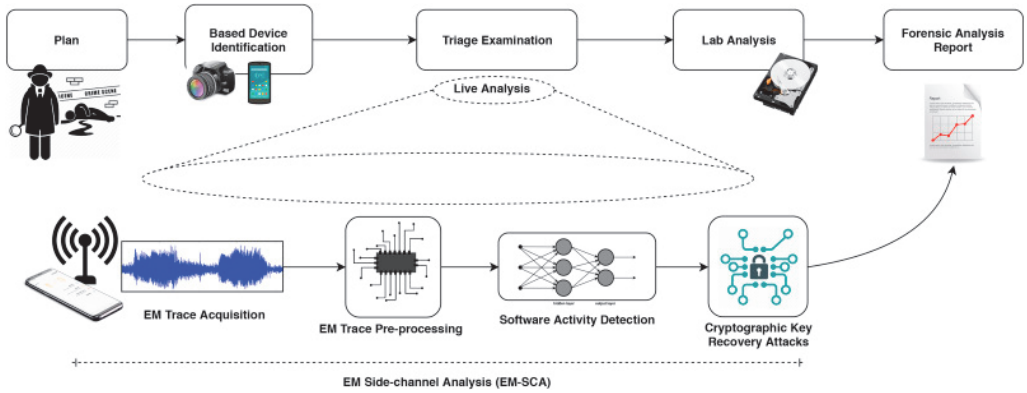
Με την έννοια ασφάλειας υλικού συνεπάγεται με την προστασία της συσκευής και του περιφερειακού υλικού από κλοπή, ηλεκτρονική εισβολή και ζημιά. Η φυσική ασφάλεια επιτόπου μπορεί να είναι εύκολη διαδικασία, όσο κρίσιμοι υπολογισμοί και η μεταβίβαση πληροφοριών γίνονται εντός «κλειστού δωματίου» και ο περιορισμός της πρόσβασης μόνο σε εξουσιοδοτημένες οντότητες. Το πρώτο εκ αυτών των χαρακτηριστικών δεν υφίσταται στις συσκευές του IoT καθώς, όπως έχει αναλυθεί στο υποκεφάλαιο 1.3, βασικό χαρακτηριστικό των συσκευών IoT είναι η απομακρυνσμένη επικοινωνία τους. Παρακάτω, θα αναλυθούν επιθέσεις που σχετίζονται με το υλικό των συσκευών που λαμβάνουν τόπο στο IoT.

2.6.1 Ψεύτικο Αντίγραφο

Η παραγωγή ψεύτικων αντιγράφων ή παραποίηση αποτελεί επίθεση όπου ο κακόβουλος παραποιεί την αρχική πνευματική ιδιοκτησία (IP). Ο εισβολέας χρησιμοποιώντας την επωνυμία του αρχικού σχεδιαστή χρησιμοποιεί παλιά σχέδια για την ανακατασκευή των IC ή IP. Σε αυτή την απειλή συνήθως, ο κακόβουλος εισάγει κυκλώματα Trojans θέτοντας σε κίνδυνο τις συσκευές ή υπηρεσίες [57]. (M. Rostami, 2014)

2.6.2 Επίθεση Πλευρικού Καναλιού

Η επίθεση πλευρικού καναλιού είναι μία δημοφιλής επίθεση όπου ο κακόβουλος μπορεί να αποκτήσει πληροφορίες και δεδομένα. Συγκεκριμένα, εκμεταλλεύεται φυσικές συμπεριφορές του υλικού των συσκευών όπως την κατανάλωση ενέργειας, τιμές χρονισμού κ.α. οι οποίες προδίδουν ευαίσθητες πληροφορίες. Οι επιτιθέμενοι συχνά εφαρμόζουν τέτοιες επιθέσεις σε κρυπτο-συστήματα, για την ανάκτηση κλειδιών που χρησιμοποιείται στα πλαίσια της επικοινωνίας. Η εξαγωγή πληροφοριών μπορεί να επιτευχθεί με ανάλυση καθυστέρησης, με μέτρηση κατανάλωσης ισχύος, με μέτρηση φωτονικών εκπομπών, με μέτρηση ηλεκτρομαγνητικών εκπομπών και από των ακουστικό θόρυβο [84]. (Du, et al., 2017)



Εικόνα 7: Επίθεση πλευρικού καναλιού[9] [84]. (Du, et al., 2017)

2.6.3 Επίθεση μέσω Αντίστροφης Μηχανικής

Η επίθεση μέσω της μεθόδου αντίστροφης μηχανικής προϋποθέτει προηγμένο εξοπλισμό και εξειδικευμένες γνώσεις από πλευράς επιτιθέμενων. Ανήκει στην κατηγορία επεμβατικών επιθέσεων ώς προς τον τύπο της.Περιλαμβάνει την ανακατασκευή IC ή IP με ενσωματωμένο ένα κακόβουλο κύκλωμα. Ο επιτιθέμενος

[9] https://www.sciencedirect.com/

ακολουθεί την αντίστροφη διαδρομή σε αντίθεση με τον παραδοσιακό σχεδιασμό IC ή IP. Η επίθεση αυτή απαρτίζεται από διάφορα στάδια. Περιλαμβάνει την ανίχνευση του μοντέλου που χρησιμοποιείται κατά τον σχεδιασμό και σύνθεση, την αφαίρεση διαφορετικών τμημάτων του σχεδιασμού ή οποία προϋποθέτει ακριβό εξοπλισμό και τέλος την παρατήρηση της λειτουργικότητας του IC ή IP. Η αξιολόγηση της συμπεριφοράς του κυκλώματος γίνεται με βάση την παρατήρηση των συνδυασμών εισόδων και εξόδων σχετικά με την αναμενόμενη συμπεριφορά. Έτσι, γίνεται η επαλήθευση της σχεδίασης επιπέδου πύλης του IC ή IP. Η εμφύτευση κακόβουλου κυκλώματος κατά τον σχεδιασμό μπορεί να απειλήσει τα συστήματα αποκαλύπτοντας σημαντικές πληροφορίες.

2.6.4 Παραβίαση Πνευματικής Ιδιοκτησίας

Η παραβίαση πνευματικής ιδιοκτησίας (IP) συντελεί επίθεση που λαμβάνει χώρα κατά την φάση σχεδιασμού IC (ολοκληρωμένων κυκλωμάτων). Οι κακόβουλοι κλέβουν τις σχεδιαστικές πληροφορίες και σε πολλές περιπτώσεις διεκδικούν το δικαίωμα κατοχής της ιδιοκτησίας της IP ή του IC. Με την επίθεση της παραβίασης πνευματικής ιδιοκτησίας κυκλοφορούν στην αγορά παράνομα IC ή IP με κακόβουλα κυκλώματα και ενσωματώνονται σε συσκευές με αποτέλεσμα να αποτελεί πρόκληση στο επίπεδο ασφαλείας.

2.6.5 Δούρειοι Ίπποι σε επίπεδο υλικού

Οι «Δούρειοι Ίπποι» σε επίπεδο υλικού (Hardware Trojan) είναι μία επίθεση όπου επιτιθέμενοι τροποποιούν ένα ολοκληρωμένο κύκλωμα ή ενσωματώνουν ένα ολοκληρωμένο κύκλωμα σε συσκευή το οποίο προκαλεί βλάβες σε μονάδες ελέγχου και παραπλάνηση επικοινωνίας. Μέσω της απειλής αυτής μπορεί να διαρρεύσουν εμπιστευτικές πληροφορίες και δεδομένα πλήττοντας το ζήτημα ασφαλείας της εμπιστευτικότητας. Οι «Δούρειοι Ίπποι» μπορούν να διαρρεύσουν ένα κρυπτογραφικό κλειδί και κωδικούς πρόσβασης μέσω της σύνδεσης των συσκευών στο διαδίκτυο [58,59]. (Karri, et al., 2010) (Tehranipoor, et al., 2010).

Είναι ιδιαίτερα δύσκολο να εντοπιστούν, καθώς συχνά παίρνουν τη μορφή ιδιαίτερα συνηθισμένων εργαλείων ή εργαλείων που απαιτούν την χειροκίνητη εγκατάσταση τους από το χρήστη ή υπάρχουν σε κάποιο υπολογιστή με τη μορφή ενός μεταφρασμένου προγράμματος που είναι δύσκολο να ελεγχθεί ώς προς την λειτουργία του.

2.6.6 Timing Attacks

Κατα τις επιθέσεις χρονισμού, όπως και στις επιθέσεις πλευρικού καναλιού, ο επιτιθέμενος μέσω στατιστικής ανάλυσης αναζητεί συσχετισμούς της τυχαίας εισόδου προς την έξοδο. Η μέθοδος της στατιστική ανάλυση λειτουργεί μόνο εάν το σύστημα συμπεριφέρεται με παρόμοιο τρόπο από εκτέλεση σε εκτέλεση με για μία κοινή είσοδο.

Ο επιτιθέμενος με τις επιθέσεις χρονισμού προσπαθεί να εκμεταλλευτεί μικρές διαφορές που παρατηρείται στο χρονοδιάγραμμα των αλγορίθμων. Για παράδειγμα, η μέτρηση του χρονισμού ενός αλγορίθμου αποκωδικοποίησης κωδικού πρόσβασης και η διερεύνηση των πρώτων εξόδων από τη ρουτίνα. Οι επιτιθέμενοι έχουν την δυνατότητα με αυτόν τον τύπο επίθεσης να παρατηρήσουν τη χρήση της προσωρινής μνήμης. Έτσι θα μπορέσουν να ανλήσουν στοιχεία για τα χαρακτηριστικά του αλγορίθμου [83]. (Lea, 2019)

Σε μία επίθεση χρονισμού, παρατηρώντας ο κρυπταναλυτής την κίνηση της πληροφορίας από και προς την CPU ή την μνήμη καθώς το hardware τρέχει τον κρυπταλγόριθμο. Ο επιτιθέμενος είναι σε θέση ακόμα και να αποκαλύψει το μυστικό κλειδί μετρώντας την τιμή του χρόνου που χρειάζεται το hardware, έτσι ώστε να ολοκληρωθούν κάποιες κρυπτογραφικές λειτουργίες, και συγκρίνοντας ακολούθως τις διαφορές των χρονικών αυτών μετρήσεων. Μετρώντας το χρόνο που απαιτείται για να εκτελεστούν οι λειτουργίες που σχετίζονται με το ιδιωτικό κλειδί, ο κακόβουλος χρήστης έχει την δυνατότητα να ανακαλύψει τους εκθέτες που χρειάζεται, να παραγοντοποιήσει τα κλειδιά του RSA και να σπάσει το κρυπτοσύστημα. Αν η μονάδα είναι ευάλωτη, τότε η επίθεση είναι υπολογιστικά απλή και συχνά χρειάζεται μόνο ένα γνωστό κρυπτογράφημα.

2.6.7 Simple Power Analysis

Η επίθεση Simple Power Analysis (SPA) αποτελεί μία μη-επεμβατική επίθεση, που όπως και στις επιθέσεις χρονισμού, ο εισβολέας μέσω στατιστικής ανάλυσης αναζητεί συσχετισμούς εισόδου-έξοδου. Η SPA επίθεση στοχεύει στην διακύμανση της ροής εντολών. Δεν θα αφήνει αποδεικτικά στοιχεία, έτσι ο κάτοχος της συσκευής δεν θα γνωρίζει ότι πραγματοποιήθηκε επίθεση. Κατα την SPA δεν απαιτείται καμία αρχική προετοιμασία για την επίθεση σε μια συσκευή.

Σε αυτό τον τύπο επίθεσης μετρά μεγάλες αλλαγές στη δυναμική ισχύ ή το ρεύμα λόγω της συμπεριφοράς ενός αλγορίθμου. Ο επιτιθέμενος μπορεί εύκολα με αυτόν τον τύπο επίθεσης να αποκτήσει δημόσια κλειδιά που χρησιμοποιούνται στα πλαίσια της επικοινωνίας. Η στατιστική ανάλυση χρειάζεται κάποιον μικρό αριθμό ιχνών για να είναι αποτελεσματική, αλλά τα ίχνη χρειάζονται υψηλό βαθμό ακρίβειας [83]. (Lea, 2019)

2.6.8 Differential Power Analysis

Η Differential Power Analysis (DPA), συντελεί μία μη-επεμβατική επίθεση, πανομοιότυπη επίθεση με αυτή του πλευρικό καναλιού και την SPA. Η DPA στοχεύει στην εξάρτηση από τα δεδομένα. Η DPA μετρά δυναμική ισχύ, αλλά μπορεί να παρατηρήσει αλλαγές που είναι πολύ μικρές για να διακριθούν απευθείας όπως στην επίθεση SPA. Όπως και η SPA, η DPA δεν αφήνει αποδεικτικά στοιχεία, με αποτέλεσμα ο κάτοχος της συσκευής να μην γνωρίζει ότι πραγματοποιήθηκε επίθεση.

Ο επιτιθέμενος έχει την δυνατότητα να εκτελέσει χιλιάδες ίχνη για να δημιουργήσει ένα σύνολο που εξαρτάται από τα δεδομένα με την έγχυση τυχαίας εισόδου σε ένα σύστημα. Τα σύνολα είναι κατά μέσο όρο και η διαφορά μεταξύ του συνόλου 0 και 1 σχεδιάζεται για να παρουσιάσει το αποτέλεσμα της τυχαίας εισόδου στην έξοδο [83]. (Lea, 2019)

2.6.9 Επιθέσεις Μηχανικής Μάθησης (ML)

Οι επιθέσεις με μηχανική εκμάθηση (ML) είναι ένας από τους πιο συνηθισμένους τύπους μη επεμβατικών επιθέσεων στο υλικό και συγκεκριμένα εναντίον PUF. Οι ML επιθέσεις απαιτούν από τον αντίπαλο να παρακολουθεί αποκλειστικά την είσοδο-έξοδο του στοχευμένου PUF. Ένα σχετικά μικρό υποσύνολο προκλήσεων μαζί με τις αντίστοιχες αποκρίσεις συλλέγονται από τον αντίπαλο, ο οποίος προσπαθεί να βρει ένα μοντέλο από την συμπεριφορά του PUF.

2.6.10 Ανάλυση ηλεκτρομαγνητικής ισχύος (EMA)

Η EMA συνιστά μία παρόμοια επίθεση με αυτή της SPA και της DPA. Σε αντίθεση με τις Power Analysis (PA) επιθέσεις παράγει τοπικές πληροφορίες πιο «στοχευμένες» που βοηθούν τον κρυπτοαναλυτή να εξάγει κλειδιά. Επιπρόσθετα, αν και συγκριτικά με τις PA επιθέσεις είναι πιο πολύπλοκες, προσπερνούν αντίμετρα υλικού όπως τις ασπίδες (shields) και τη τυχαιοποιημένη λογική, γεγονός που τις καθιστά πιο επικίνδυνες.

ΚΕΦΑΛΑΙΟ 3 : PUF ΚΑΙ IOT

Η PUF αποτελεί μία φυσική οντότητα που ενσωματώνεται και εφαρμόζεται σε φυσικές δομές που χαρακτηρίζονται από υψηλές απαιτήσεις ασφαλείας. Λειτουργικά, για την εγκαθίδρυση ασφάλειας, εκμεταλλεύεται τις φυσικές ιδιότητες των συστημάτων για σκοπούς ελέγχου. Πρώτες αναφορές πάνω στις PUF χρονολογούνται το 1983 από τον Bauder και το 1984 από τον Simmons. Το 1992 οι Naccache και Fremanteau παρείχαν ένα σχέδιο ταυτότητας για κάρτες μνήμης για να φτάσουμε στο σημείο το 2002 να περιγραφεί από την επιστημονική κοινότητα το πρώτο ολοκληρωμένο PUF, το οποίο είναι ενσωματωμένο σε ολοκληρωμένο κύκλωμα (IC)[38]. (Halak, et al., 16-19 Oct. 2016)

3.1 PUF

Η ανάπτυξη των ηλεκτρονικών συσκευών κατέστησε ανησυχητική την ασφάλεια του υλικού τους. Κατά την ανάπτυξη ηλεκτρονικών συσκευών παρουσιάστηκαν κίνδυνοι παραχαράξεων και κλωνοποίησης κυκλωμάτων από κακόβουλα άτομα, τα οποία με προηγμένα εργαλεία και εξειδικευμένες γνώσεις επεμβαίνουν στο υλικό. Μια PUF αποτελεί ένα φυσικό αντικείμενο που για μια δεδομένη είσοδο (πρόκληση), παρέχει μία καθορισμένη έξοδο (απόκριση). Ουσιαστικά, η έξοδος είναι το «ψηφιακό δακτυλικό αποτύπωμα» που χρησιμεύει ως ταυτότητα. Τα PUFs βασίζονται ως επί το πλείστον σε μοναδικές φυσικές διαταραχές που συμβαίνουν φυσικά κατά την κατασκευή ημιαγωγών. Το PUF ενσωματώνεται σε ένα ολοκληρωμένο κύκλωμα παρέχοντάς του ασφάλεια απέναντι σε απειλές κλωνοποίησης ή παραχάραξης [61]. (Babaei, et al., 2019).

Ένα κύκλωμα με ενσωματωμένη την φυσική οντότητα PUF αντιδρά με απρόβλεπτο τρόπο, λόγω της περίπλοκης αλληλεπίδρασης του ερεθίσματος με τη φυσική μικροδομή της συσκευής. Η μικροδομή εξαρτάται εξ' ολοκλήρου από ιδιότητες υλικού, οι οποίες είναι απρόβλεπτες και προέρχονται κατά την φάση κατασκευής της. Το ερέθισμα που δέχεται η δομή ονομάζεται «πρόκληση» και η απάντηση του PUF στην πρόκληση αυτή ονομάζεται «απόκριση». Το ζεύγος πρόκληση-απόκριση ή CRP είναι μοναδικό, δηλαδή για μία συγκεκριμένη πρόκληση υπάρχει συγκεκριμένη απόκριση. Η μοναδικότητα αυτή προσδίδει ένα μοναδικό ισχυρό κρυπτογραφικό κλειδί από τη φυσική μικροδομή. Η υλοποίηση των PUFs περιλαμβάνει μικρές απαιτήσεις σε επένδυση υλικού και η χρήση τους έχει μειωμένο κόστος όσον αφορά στην κατανάλωση ενέργειας και τους πόρους [62]. (Burg, et al., 2018).

3.1.1 Αδύναμες και ισχυρές υλοποιήσεις PUFs

Τα επίπεδα αντοχής των PUFs, όσον αφορά στην ισχύ τους, μπορούν να χαρακτηριστούν αδύναμα ή ισχυρά. Αυτή η ισχύς εξαρτάται άμεσα από τον αριθμό των ζευγών CRPs που μπορούν να δημιουργηθούν από μία και μόνο συσκευή. Τα αδύναμα PUF υποστηρίζουν μικρό αριθμό προκλήσεων και αποκρίσεων. Λόγω του μικρού πλήθους ζευγών, εάν κακόβουλο άτομο αποκτήσει φυσική πρόσβαση θα έχει την δυνατότητα να διαβάσει αυτά τα δεδομένα από την συσκευή. Καλή πρακτική αποτελεί η χρήση αδύναμων PUFs για την Αποθήκευση κρυπτογραφικών κλειδιών, καθώς και για τεχνικές ελέγχου ταυτότητας οντοτήτων.

Τα ισχυρά PUFs υποστηρίζουν μεγαλύτερο πλήθος ζευγών προκλήσεων-αποκρίσεων. Ο κακόβουλος χρήστης ακόμα και αν αποκτήσει πρόσβαση στο PUF αδυνατεί να διαβάσει και να καταγράψει τις πληροφορίες. Κάθε ζεύγος πρόκλησης απόκρισης χρησιμοποιείται μία και μοναδική φορά, γεγονός που περιορίζει τους κινδύνους από υποκλοπές και ενθαρρύνει την ασφαλή επικοινωνία.

3.1.2 Τυχαιότητα PUFs

Η τυχαιότητα στα πλαίσια των αποκρίσεων των φυσικών οντοτήτων που προκύπτουν από τα ερεθίσματα (προκλήσεις) προκαλεί την μοναδικότητα. Η τυχαιότητα ανάλογα με τον τρόπο που προκύπτει διακρίνεται σε ρητή τυχαιότητα και σιωπηρή τυχαιότητα. Η ρητή τυχαιότητα προκύπτει από την εξωτερική παρεμβολή μέσω της εφαρμογή επιπρόσθετων βημάτων, τα οποία δημιουργούν τυχαιοποίηση ως προς την απόκλιση της φυσικής δομής. Η σιωπηρή τυχαιοποίηση προκύπτει φυσικά από παραλλαγές σε τυποποιημένες διαδικασίες κατασκευής. Η σιωπηρή τυχαιότητα που προκύπτει από PUFs δεν απαιτεί πρόσθετα βήματα επεξεργασίας που συνεπάγεται επιπρόσθετο κόστος σε αντίθεση με ρητή τυχαιότητα. Επιπρόσθετα, η σιωπηρή τυχαιοποίηση δημιουργεί παραλλαγές βασισμένες σε τυπικές διαδικασίες από την κατασκευή, γεγονός που προσφέρει ακεραιότητα των τυχαίων χαρακτηριστικών από εξωγενείς οντότητες.

3.1.3 Αξιολόγηση PUFs

Μία συσκευή μπορεί να είναι είτε ενδογενής είτε εξωγενής ανάλογα με την αξιολόγηση του μηχανισμού στο εσωτερικό της. Κατά την ενδογενή αξιολόγηση, ένα εγγενές PUF έχει τυχαιότητα που πραγματοποιείται από έμμεσο τρόπο και αξιολογεί εσωτερικά εντός της δομής. Τα μέσα μέτρησης και ανίχνευσης βρίσκονται ενσωματωμένα στην συσκευή με αποτέλεσμα να μην εκτίθεται η απόκριση προς τα έξω. Το χαρακτηριστικό αυτό προσδίδει ανθεκτικότητα έναντι επιθέσεων man in the middle και πλευρικού καναλιού. Η εξωγενής αξιολόγηση πραγματοποιείται εξωτερικά της δομής γεγονός που την καθιστά πιο ευαίσθητη σε επιθέσεις από κακόβουλους χρήστες.

3.1.4 Μονάδες ποιότητας PUFs

Για την αξιολόγηση της ποιότητας ενός PUF υπάρχουν πολλές μετρικές που χρησιμοποιούνται. Βασικές μετρήσιμες ποσότητες αποτελούν η μοναδικότητα που σχετίζεται με την παραγωγή μοναδικών αναγνωριστικών και η αξιοπιστία που συνδέεται με την ικανότητα των PUFs να παράγουν συνεπείς αποκρίσεις για κάθε πρόκληση στην δομή.

Η μοναδικότητα αποτελεί ένα μέτρο σχετικά με την δυνατότητα μίας συσκευής να δημιουργεί μοναδικά αναγνωριστικά. Η εκτίμηση της ποσότητας αυτής προϋποθέτει την χρήση της απόστασης Hamming μεταξύ των τσιπ ανάμεσα σε σύνολο αποκρίσεων της ίδιας δομής PUF σε διαφορετικές συσκευές. Η απόσταση Hamming αναλαμβάνει σημαντικό ρόλο στην αξιολόγηση της ποιότητας ενός σχεδιασμού PUF. Ενδεικτικά, η μετρήσιμη ποσότητα της μοναδικότητας πρέπει να τείνει στο 50%. Τιμές κοντά σε αυτή τη ποσότητα συνεπάγονται ότι κάθε συσκευή PUF έχει μια μοναδική απόκριση σε πρόκληση.

Το μέτρο της ικανότητας του PUF να παράγει μια συνεπή απόκριση για μία πρόκληση, παρά την διακύμανση του περιβάλλοντος όπου λειτουργεί, σχετίζεται άμεσα με την έννοια της αξιοπιστίας. Οι διακυμάνσεις αυτές σχετίζονται με την τάση τροφοδοσίας και την θερμοκρασία. Σε αυτή την περίπτωση χρησιμοποιείται η απόσταση Hamming intra-chip, η οποία ιδανικά πρέπει να είναι 0%. Η απόκριση HDintra δημιουργείται σε θερμοκρασία δωματίου. Η τιμή της αξιοπιστίας ιδανικά θα πρέπει να είναι στο 100%. Συνεπώς, η απόκριση PUF παραμένει η ίδια παρά από το θόρυβο και τη μεταβλητότητα των συνθηκών λειτουργίας του.

$$(\text{Μοναδικότητα}) = \frac{1}{\binom{l}{2}} \sum_{i=1}^{l-1} \sum_{j=i+1}^{l} HD(R_i, R_j) * 100\% \quad (1)$$

$$(\text{Αξιοπιστία}) = 100 - \frac{1}{n*(l-1)} \sum_{j=2}^{l} \sum_{n=1}^{n} HD(R_{i,k}, R_{j,k}) \quad (2)$$

Εικόνα 8: Τύποι μονάδων ποιότητας PUF.

3.2 ΤΥΠΟΙ PUFS

Στα πλαίσια κατασκευής μίας PUF χρησιμοποιούνται διάφορα στοιχεία για την εξαγωγή δακτυλικών αποτυπωμάτων από μία συσκευή. Ως προς την τυχαιότητα, που αποτελεί χαρακτηριστικό που προσφέρει μοναδικότητα (μέτρο αξιολόγησης ποιότητας PUFs), τα PUFs διακρίνονται σε οπτικά PUFs και PUFs επίστρωσης. Τα PUFs επίστρωσης κατασκευάζονται γεμίζοντας το διάστημα ανάμεσα ενός δικτύου μεταλλικών καλωδίων πάνω από ένα ολοκληρωμένο κύκλωμα, επεμβατικά με τυχαίο τρόπο με διηλεκτρικά σωματίδια. Ο τύπος αυτός χρησιμοποιείται ως RFID tags τεχνολογία, καθώς και στο ανώτερο στρώμα ολοκληρωμένων κυκλωμάτων συσκευών θωρακίζοντας τα συστήματα από επιθέσεις inspection (επιθεώρησης). Τα οπτικά PUFs χρησιμοποιούν τις φυσικές παραμέτρους ενός διαφανούς υλικού, πάνω στο οποίο σωματίδια φωτός διασκορπίζονται με τυχαίο και ανεξέλεγκτο τρόπο. Η φυσική ιδιότητα του διαφανούς υλικού συμπεριφέρεται τυχαία όταν πέφτει μία ακτίνα λέιζερ προσφέροντας, κατά αυτόν τον τρόπο μοναδικότητα.

Για την παραγωγή τυχαίων απαντήσεων σε ερεθίσματα, οι τεχνολογίες βασίζονται στις εγγενείς παραλλαγές. Οι εγγενείς παραλλαγές στην διαδικασία παραγωγής ολοκληρωμένων κυκλωμάτων προσδίδουν υψηλότερα επίπεδα ασφαλείας, καθώς η λειτουργικότητα του PUF πυριτίου εξαρτάται μόνο από το εσωτερικό της δομής του. Οι φυσικές διαταραχές της οντότητας PUF ανάλογα με τον σχεδιασμό και την κατασκευή του προσφέρουν τυχαιότητα και μοναδικότητα μέσω διαφορετικών ρευμάτων διαρροής ή μέσω καθυστερήσεων. Συμβατικές υλοποιήσεις PUFs με καθυστέρηση αποτελούν το Arbiter PUF και το Ring Oscillator (RO) PUF.

Παράμετροι	**RO PUF**	**SRAM**	**Arbiter PUF**
Τυχαιότητα	46 %	49.65 %	30 %
Μοναδικότητα	47.31 %	50.1 %	40 %
Αξιοπιστία	92 %	83 %	100 %

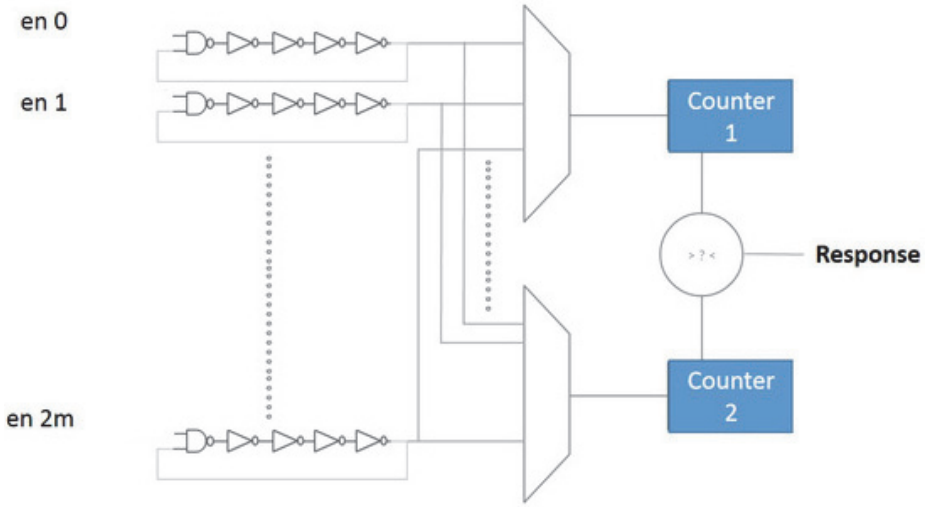
Πίνακας 1: Σύγκριση μετρήσεων απόδοσης των διαφορετικών PUFs[10].

[10] https://ieeexplore.ieee.org/document/9221357

3.2.1 Ring Oscillator PUF

Οι ταλαντωτές δακτυλίου (Ring Oscillator-RO) αποτελούν βασικό δομικό στοιχείο των PUFs. Σε συνδυασμό με τον συγκριτή, τους πολυπλέκτες και τους μετρητές δίνουν την συμπεριφορά των PUFs. Οι RO ταλαντεύονται σε μοναδικές συχνότητες ανάλογα με τα χαρακτηριστικά καθυστέρησης δίνοντας την ζητούμενη τυχαιότητα που προσδοκάται από την χρήση της PUF, η οποία σχετίζεται με φυσικές διαταραχές. Η συμπεριφορά του PUF για την παραγωγή τυχαιότητας στηρίζεται σε δύο μετρητές, οι οποίοι μετρούν τον αριθμό των ταλαντώσεων των ταλαντωτών δακτυλίου σε σταθερό χρονικό διάστημα. Στο τέλος του διαστήματος αυτού, οι έξοδοι των μετρητών συγκρίνονται μεταξύ τους από τον συγκριτή και ο μετρητής κάτοχος της μέγιστης τιμής ορίζει την έξοδο του PUF [68]. (Cao, και συν., 2015).

Τα RO-PUFs από την άλλη, παρουσιάζουν ευαισθησία στην κλωνοποίηση χρησιμοποιώντας ηλεκτρομαγνητική ανάλυση. Οι ηλεκτρομαγνητικές ενέσεις μπορούν να κλειδώσουν τα κύτταρα RO. Αυτό το γεγονός, χρίζει προβληματική την χρήση αυτής της τεχνολογίας στο IoT, που είναι υψίστης σημασίας το απόρρητο, αφού μεταβιβάζονται ευαίσθητα προσωπικά δεδομένα [100]. (Michailidis, Kogias, & Voyiatzis, 2020)



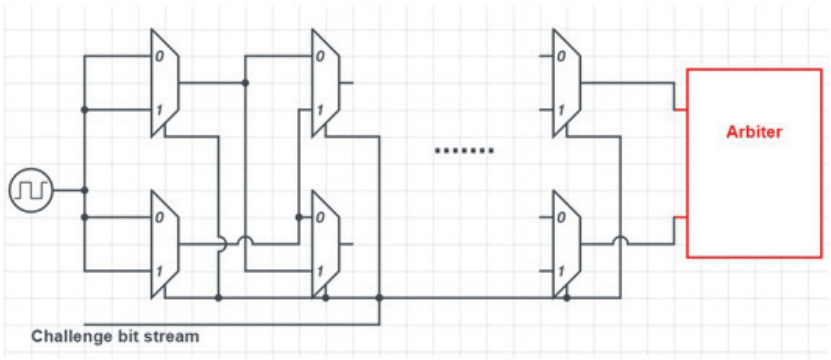
Εικόνα 9: Ring oscillator αρχιτεκτονική[11].

[11] https://doi.org/10.3390/s19143208

3.2.2 Arbiter PUF

Η PUF που βασίζεται σε Arbiter αποτελεί άλλον έναν τύπο PUF, όπως ο RO, που κατατάσσεται στις PUF με καθυστέρηση. Ο Arbiter λειτουργεί σαν «διαιτητής», ο οποίος ανάλογα με την χρονική στιγμή που θα φθάσει μία ψηφιακή διαδρομή σε εκείνον, εξάγει μία αντίστοιχη τιμή τύπου 0 ή 1. Ουσιαστικά, ένα PUF δέχεται σαν είσοδο δύο ψηφιακές διαδρομές την ίδια χρονική στιγμή. Ο «κριτής» (διαιτητής) είναι στοιχείο εγγενή, ο οποίος είναι αρμόδιος για την τυχαία απόκριση του συστήματος. Η τυχαιότητα οφείλεται στην επιλογή του Arbiter του chip σχετικά με την ταχύτερη διαδρομή παράγοντας αντίστοιχο δυαδικό ψηφίο [61]. (Babaei, και συν., 2019)

Παρόλα αυτά, οι επιθέσεις μοντελοποίησης της υποκείμενης συμπεριφοράς απόκρισης προκαλεί αβεβαιότητα σχετικά με την εφαρμογή τους. Ο επιτιθέμενος με αλγόριθμους που μαθαίνουν αυτόματα μια πολύπλοκη συμπεριφορά από περιορισμένο αριθμό παρατηρήσεων, είναι σε θέση να γενικεύσει τις υποκείμενες αλληλεπιδράσεις από αυτά τα δείγματα. Κατάλληλες τεχνικές ML θα μπορούσαν να μάθουν αυτήν τη συμπεριφορά από ένα σχετικά μικρό εκπαιδευτικό σύνολο γνωστών CRP [101]. (Hospodar, Maes, & Verbauwhede, 2012)



Εικόνα 10: Arbiter PUF αρχιτεκτονική[12].

[12] https://www.mdpi.com/

3.2.3 SRAM PUF

Τα SRAM PUF βασίζονται στη μνήμη, χρησιμοποιώντας τα chip μνήμης που είναι διαθέσιμα σε διαφορετικές συσκευές. Έτσι, μπορούν εύκολα να ενσωματωθούν σε οποιαδήποτε συσκευή, για την εγκαθίδρυση ασφάλειας σε ένα δίκτυο που βασίζεται σε PUF. Η αρχιτεκτονική SRAM PUF προσδίδει αξιοπιστία και αποτελεί μία ιδιαίτερα σημαντική τεχνολογία στα πλαίσια της ασφάλειας. Βασίζεται στις καταστάσεις ενεργοποίησης των μπλοκ SRAM. Λειτουργικά, καθένα από τα κελιά έχει αρχικά μία δυαδική τιμή 0 ή 1. Η κατάσταση αυτή θα διαφέρει από συσκευή σε συσκευή. Η τυχαιότητα των καταστάσεων ενεργοποίησης αποτελεί πηγή εντροπίας προσφέροντας μοναδικότητα. Στην δημιουργία ζεύγους πρόκλησης-απόκρισης συμβάλλουν η διεύθυνση και η τυχαία αρχική τιμή του κελιού.

Ωστόσο, παραλλαγές τιμών (π.χ. μέσω αστάθειας θερμοκρασίας) έχουν μεγάλο αντίκτυπο στην λειτουργία ενός SRAM, συμπεριλαμβανομένης της μείωσης της αξιοπιστίας και της απόδοσης μειώνοντας τα περιθώρια θορύβου. Αυτές οι παραλλαγές, επηρεάζουν την κλίση κάθε κελιού και παρέχουν το δακτυλικό αποτύπωμα που απαιτείται για τη χρήση του SRAM ως ασαφούς αναγνωριστικού. Επιπρόσθετα, οι τρωτότητα αυτής της κατηγορίας PUF μπορεί να γίνει αντικείμενο προς εκμετάλλευση κακόβουλων χρηστών οι οποίοι μπορούν να επιτεθούν σε ένα SRAM PUF πιέζοντας μεμονωμένα bits σε συγκεκριμένες τιμές. Έτσι, μπορεί να προκαλέσει σημαντικές αλλαγές στο δακτυλικό αποτύπωμα ενός SRAM [102]. (Roelke & Stan, 11-13 July 2016)

3.3 ΧΡΗΣΗ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ PUF ΣΤΟ IOT

Οι συσκευές που απαρτίζουν το IoT δημιουργούν ακούσια ένα τεράστιο αριθμό ευαίσθητων δεδομένων. Λόγω της δικτυωμένης φύσης του σε συνδυασμό με την σημασία της ασφαλούς μεταβίβασης των δεδομένων η ασφάλεια του αποτελεί πρωταρχική ανησυχία. Οι PUFs έχουν αναδειχθεί ως μία πολλά υποσχόμενη και ελαφριά λύση ελέγχου ταυτότητας, αντί της παραδοσιακής κρυπτογραφίας. Ωστόσο,

οι συμβατικές υλοποιήσεις PUFs έχουν βρεθεί ευάλωτες σε πολλές επιθέσεις. Αυτά τα PUF είναι ευάλωτα σε επιθέσεις πλευρικών καναλιών επειδή εκπέμπουν πληροφορίες λόγω θερμότητας ως αποτέλεσμα να μην είναι κατάλληλες για το IoT. Επιπρόσθετα, η εφαρμογή της PUF σε συστήματα IoT αποτελεί πρόκληση, λόγω της περιορισμένης χρήσης πόρων των ενσωματωμένων συσκευών [67]. (Babaei, και συν., 2019)

Το IoT αποτελείται ως επί το πλείστον από διασυνδεδεμένες συσκευές που τοπολογικά βρίσκονται σε απομακρυσμένα περιβάλλοντα. Η ανάπτυξη του IoT σε απομακρυσμένα περιβάλλοντα χαρακτηρίζεται από ελάχιστη προστασία. Επομένως, πιθανή πρόσβαση κακόβουλων χρηστών σε αυτές τις συσκευές συνεπάγεται συνήθως με συλλογή ζευγών προκλήσεων-αποκρίσεων. Τις πληροφορίες αυτές μπορεί να τις συλλέξουν οι εισβολείς από επιθέσεις πλευρικών καναλιών, στις οποίες οι PUF εμφανίζουν ευαισθησία. Η συλλογή αυτών των δεδομένων επιτρέπει σε έναν αντίπαλο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο IoT. Αυτό, γιατί μπορεί αποκτώντας αυτές τις πληροφορίες να μιμηθεί απαντήσεις PUF σε αυθαίρετες προκλήσεις [55,56]. (Rohatgi, 2009) (Schlosser, et al., 2013).

Οι κλασικές αρχιτεκτονικές PUF, παρά την δυνατότητα να παράγουν δακτυλικά αποτυπώματα, παρουσιάζουν ευαισθησία με επιθέσεις μηχανικής εκμάθησης. Η μηχανική εκμάθηση (ML) έχει έναν ιδιαίτερα σημαντικό ρόλο στο IoT και στο Cloud. Η χρήση βέβαια της ML σε IoT περιβάλλοντα παρουσιάζει προκλήσεις ασφαλείας, αφού επιτιθέμενοι μπορούν να χειραγωγήσουν τα δεδομένα που παράγει η μηχανική εκμάθηση παραβιάζοντας τις μετρήσεις των διασυνδεδεμένων αισθητήρων του IoT. Έτσι, μειώνουν σημαντικά την απόδοση των συστημάτων. Ο επιτιθέμενος μπορεί να προκαλέσει ακόμα μεγαλύτερη βλάβη στο σύστημα με την εισαγωγή backdoors («πίσω πόρτας») και με την εισαγωγή Trojans. Οι νεότερες αρχιτεκτονικές έχουν σημειώσει σαφή πρόοδο στην ανάπτυξη ανθεκτικότητας έναντι τέτοιων προκλήσεων. (Halak, και συν., 16-19 Oct. 2016)

Εν κατακλείδι, βασικό πρόβλημα στα πλαίσια της αξιοπιστίας των PUFs προκύπτει από την γήρανση των τρανζίστορ CMOS της δομής τους. Η γήρανση, μακροπρόθεσμα υποβαθμίζει τα ολοκληρωμένα κυκλώματα προκαλώντας τους διαταραχές στις ηλεκτρικές παραμέτρους των CMOS συσκευών. Το αντίκτυπο μπορεί να είναι μεγάλο, όσον αφορά στην αξιοπιστία του PUF. Οι αποκρίσεις των

PUF από προκλήσεις μπορεί να περιλαμβάνουν σφάλματα λόγω της θερμοκρασίας, γεγονός που υποβαθμίζει την PUF ως προς την αξιοπιστία της.

3.4 ΛΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ PUF

Η έλλειψη καθολικής αρχής πιστοποιητικού ρίζας καθιστά πολύ δύσκολη την ανάπτυξη ασφαλών συστημάτων μέσω κρυπτο-συστημάτων δημοσίου κλειδιού για τον έλεγχο ταυτότητας και για την εξουσιοδότηση για το IoT. Η πιστοποίηση μίας οντότητας στο IoT αποτελεί δύσκολη διαδικασία, καθώς ο αριθμός των οντοτήτων τείνει να αυξάνει εκθετικά. Ο έλεγχος ταυτότητας και εξουσιοδότησης αποτελούν μεθόδους που αποτρέπουν επιθέσεις εισβολέων, διατηρώντας τα βασικά ζητήματα ασφαλείας στο IoT. Επομένως, κρίνεται ιδιαίτερα σημαντικό προτέρημα η ενσωμάτωση τέτοιων ασφαλών μηχανισμών.

Υπάρχουν γενικά δύο κατηγορίες εφαρμογών ασφαλείας για την ανάπτυξη τέτοιων μηχανισμών στα πλαίσια της ασφάλειας των IoT. Επιπλέον, οι συσκευές του IoT τροφοδοτούνται κυρίως από μπαταρίες και χρησιμοποιούν CPU χαμηλής ισχύος με χαμηλό ρυθμό ρολογιού. Κατά τον σχεδιασμό συσκευών IoT δίνεται έμφαση στον περιορισμό της μνήμης RAM και Flash. Η κατασκευαστική ιδιαιτερότητα των συσκευών αυτών οφείλεται στο γεγονός ότι εταιρείες στοχεύουν στο περιορισμό ισχύος, του κόστους και μεγέθους των συσκευών IoT, καθώς και στην διατήρηση ποιότητας, ώστε οι συσκευές είναι αποδοτικές. Αυτό έχει ως αποτέλεσμα δημοφιλείς και συμβατικοί κρυπταλγόριθμοι, οι οποίοι απαιτούν γρήγορους υπολογισμούς και σχετικά μεγάλες απαιτήσεις σε μνήμη να μην μπορούν να χρησιμοποιηθούν στις συσκευές του IoT.

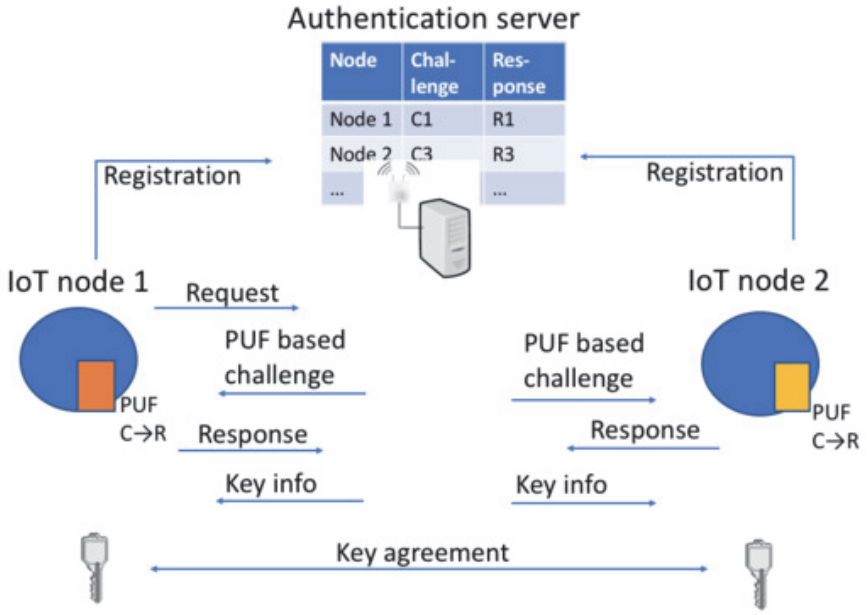
Ωστόσο, η PUF αποτελεί λύση σε ζητήματα ασφαλείας, καθώς ενσωματώνουν την διαδικασία ελέγχου ταυτότητας και εξουσιοδότησης, και παρέχουν λύση σε θέματα απορρήτου με διαδικασίες κρυπτογράφησης.

Ο έλεγχος ταυτότητας και η εξουσιοδότηση δημιουργούν κλίμα εμπιστοσύνης σε μία συσκευή IoT. Η χρήση PUF για την παροχή αυτών των διαδικασιών ασφαλείας είναι μία απλή και ελαφριά λύση, όσον αφορά στην ισχύ. Σε πρώτη φάση εφαρμόζεται από τρίτο αξιόπιστο μέρος μία σειρά προκλήσεων στην συσκευή IoT και οι αποκρίσεις της αποθηκεύονται σε βάση δεδομένων. Σε δεύτερη φάση επαληθεύεται η συσκευή επαληθεύοντας τα ζεύγη προκλήσεων και αποκρίσεων. Η επαλήθευση επιτυγχάνεται με την επιλογή μίας τυχαίας πρόκλησης και την παρατήρηση της συμπεριφοράς της συσκευής, εάν συμπεριφέρεται με βάση τα στοιχεία της ασφαλούς βάσης δεδομένων. Η χρήση PUF αποτελεί και «ασπίδα» σε επιθέσεις «man in the middle», αφού μία πρόκληση χρησιμοποιείται μία φορά. Η επαναχρησιμοποίηση θα αποτελούσε ευπάθεια, διότι οι επιτιθέμενοι θα μπορούσαν να «ξεγελάσουν» τον μηχανισμό ασφάλειας εάν γνώριζαν την συμπεριφορά του σε προκλήσεις.

Οι ενσωμάτωση PUFs συσκευών προασπίζουν τα βασικά ζητήματα ασφαλείας, την ιδιωτικότητα και την εμπιστευτικότητα. Στα παραδοσιακά ψηφιακά συστήματα, η απεριόριστη ισχύ και τα μεγάλα ενεργειακά αποθέματα επιτρέπουν την χρήση συμβατικών κρυπτογραφικών αλγορίθμων επιτυγχάνοντας τα δύο βασικά ζητήματα ασφαλείας (ιδιωτικότητα και εμπιστευτικότητα). Λόγω των ιδιαίτερων χαρακτηριστικών των συσκευών PUFs, τα ζητήματα της ιδιωτικότητας και της εμπιστευτικότητας μπορούν να διατηρηθούν με την εφαρμογή των συσκευών PUFs. Οι PUFs επιτρέπουν την δημιουργία κλειδιών κρυπτογράφησης, η οποία αποφεύγει την ανάγκη Αποθήκευσης κλειδιών στο chip. Το χαρακτηριστικό αυτό ενδείκνυται για συσκευές IoT που χαρακτηρίζονται από περιορισμένες μνήμες, επειδή δεν απαιτεί πρόσθετο χώρο Αποθήκευσης. Επιπλέον, η λειτουργικότητα αυτή καθιστά τους κόμβους του IoT λιγότερο επιρρεπής σε επεμβατικές επιθέσεις στα κανάλια. Ωστόσο, λόγω του θορύβου, οι αποκρίσεις των PUF μπορεί να εμφανίζουν διαφορετικότητα σε κάθε αξιολόγηση. Κρίνεται σημαντική η διασφάλιση σταθερών αποκρίσεων σε σειρά προκλήσεων των PUFs προκειμένου να παραχθεί το κλειδί κρυπτογράφησης. Η διαδικασία της κρυπτογράφησης συμβάλλει στην εξασφάλιση της ιδιωτικότητας και της εμπιστευτικότητας. Λειτουργικά, σε πρώτο στάδιο το PUF δημιουργεί μια απόκριση για μία καθορισμένη πρόκληση. Η απόκριση εφαρμόζεται με διόρθωση σφάλματος και σε συνδυασμό με bit συνδρόμου, ώστε τυχόν θόρυβοι να μην διαταράζουν την διαδικασία κρυπτογράφησης. Σε τελικό στάδιο, το κλειδί

κρυπτογράφησης είναι τύπου XOR, δημιουργεί «κρυπτοκείμενο» από το απλό κείμενο (plain text). Η αποκρυπτογράφηση της πληροφορίας πραγματοποιείται από πλευρά δέκτη που χρησιμοποιεί τα ζεύγη προκλήσεων αποκρίσεων για την δημιουργία του κλειδιού αποκρυπτογράφησης. Έτσι, μία συσκευή περιορισμένων πόρων, με ενσωματωμένο PUF στο IoT μπορεί να λειτουργήσει τόσο ως αποστολέας αλλά και ως δέκτης πληροφοριών. Η αμφίδρομη επικοινωνία απαιτεί από πλευράς πομπού την μετάδοση πρόκλησης και bit συνδρόμου, τα οποία θα συνεισφέρουν στον υπολογισμό του κλειδιού και στην κρυπτογράφηση των δεδομένων που θέλει να μεταδώσει [66]. (Braeken, 2018).

Μια συσκευή βασισμένη σε PUF «γεννά» ένα κλειδί με βάση τις μοναδικές ιδιότητες κάθε υλικού πυριτίου. Η χρήση μιας συσκευής που βασίζεται σε PUFs για την ασφάλεια δεδομένων, εμποδίζει εσωτερικούς χρήστες εντός του δικτύου στο IoT που έχουν πρόσβαση σε κλειδιά, να παραβιάζουν συσκευές. Με τα ιδιωτικά και δημόσια κλειδιά που δημιουργούνται, ξεκινά η επικοινωνία κατά την οποία ένας διακομιστής cloud διαθέτοντας δημόσια κλειδιά στέλνει σε κάθε συσκευή ένα ερέθισμα (πρόκληση). Αν η απάντηση (απόκριση) είναι ορθή, βάσει τα προκαθορισμένα ζεύγη, τότε ανταλλάσονται πληροφορίες βασιζόμενη στην κρυπτογράφηση πληροφοριών με τα ιδιωτικά κλειδιά. Με αυτόν τον τρόπο επιτυγχάνεται ασφάλεια στα πλαίσια των επικοινωνιών [45]. (Gassend, et al., November 2002).



Εικόνα 11: Πρωτόκολλο αυθεντικοποίησης βασισμένη σε PUF στο Διαδίκτυο των Πραγμάτων[13]

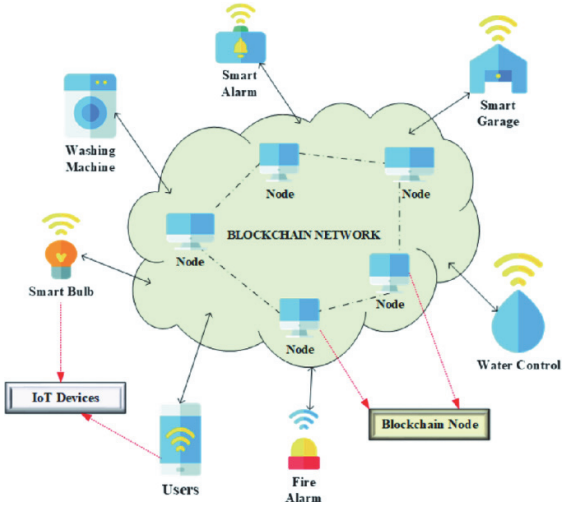
3.5 ΣΥΝΔΥΑΣΤΙΚΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΜΕ PUF

Οι συσκευές που απαρτίζουν το IoT αυξάνονται ραγδαία χρόνο με τον χρόνο, δημιουργώντας ακούσια μεγάλο αριθμό ευαίσθητων δεδομένων. Η επικοινωνία των συσκευών IoT μέσω του δημόσιου Διαδικτύου καθιστά τα μεταβιβαζόμενα δεδομένα ευαίσθητα σε πολλές κυβερνοεπιθέσεις. Μια αποτελεσματική προσέγγιση blockchain που βασίζεται στο μυστικό υπολογιστικό μοντέλο μιας PUF είναι καλή λύση για επιθέσεις που τείνουν να βλάψουν το απόρρητο. Η προστασία των δεδομένων συγκροτεί την μεγαλύτερη πηγή ανησυχίας, καθώς αποτελούν κύριο στόχο κυβερνοεγκληματιών. (Patil, και συν., 2020).

[13] https://www.mdpi.com/2073-8994/10/8/352

Το blockchain είναι μία τεχνολογία καταγραφής πληροφοριών που συνδυάζεται με το IoT, καθιστώντας ασφαλή την πραγματοποίηση συναλλαγής δεδομένων μεταξύ των διασυνδεδεμένων συσκευών. Η επαλήθευση πομπού και δέκτη στα πλαίσια των συναλλαγών καταγράφονται σε μία ασφαλή βάση δεδομένων στην οποία επαληθεύονται οι διασυνδεδεμένες πλευρές και εισάγονται σε ένα κατανεμημένο καθολικό καταγραφής πληροφοριών. Με την ενσωμάτωση της τεχνολογίας αυτής στο IoT επιτρέπεται σε συσκευές δικτυωμένες να στέλνουν δεδομένα σε ιδιωτικά δίκτυα blockchain δημιουργώντας ανθεκτικές σε παραβιάσεις εγγραφές κοινών δεδομένων [73]. (Patil, και συν., 2020).

Ο συνδυασμός blockchain και PUF εγγυάται την προέλευση των δεδομένων και την ακεραιότητα των δεδομένων σε δίκτυα IoT. Τα PUFs, όπως έχει αναφερθεί, παρέχουν μοναδικά δακτυλικά αποτυπώματα υλικού, προσφέροντας ασφάλεια στα πλαίσια τις επικοινωνίας, αφού μπορούν να χρησιμοποιηθούν κατά τον έλεγχο ταυτότητας και κατά την κρυπτογράφηση. Το blockchain παρέχει ένα αποκεντρωμένο ψηφιακό καθολικό μπλόκ που αποτελεί ικανό αντίμετρο σε επιθέσεις παραβίασης δεδομένων. Έτσι συνδυαστικά, μπορούν να συγκροτήσουν θεμέλιο ασφαλείας διατηρώντας το απόρρητο και συνεπώς την εμπιστευτικότητα των δεδομένων [53]. (Wen, και συν., 2019).



Εικόνα 12: Πρωτόκολλο ασφαλούς ελέγχου ταυτότητας βάση Blockchain-PUF στο IoT[14] [83]. (Patil, και συν., 2020)

[14] https://link.springer.com/

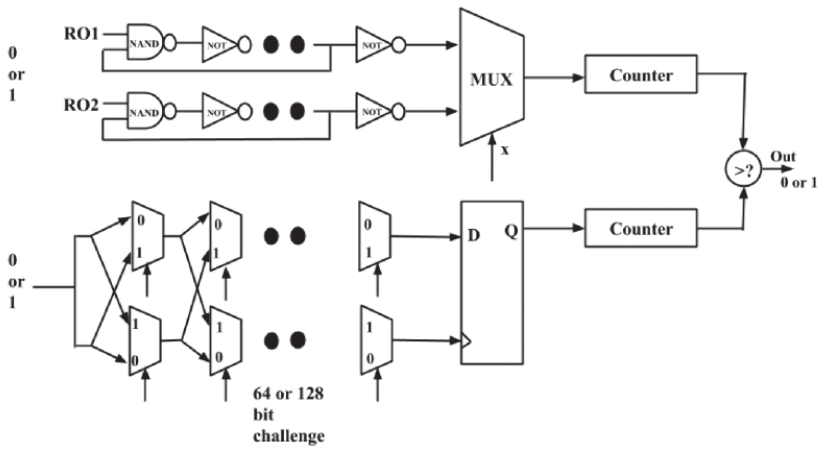
ΚΕΦΑΛΑΙΟ 4 : ΕΙΔΙΚΑ ΣΧΕΔΙΑΣΜΕΝΕΣ PUF ΓΙΑ ΤΟ IOT

Το IoT διακρίνεται από πληθώρα διασυνδεδεμένων συσκευών περιορισμένης μνήμης, μικρής κατανάλωσης ενέργειας, περιορισμένης υπολογιστικής ισχύς και περιορισμένης χρήσης κόμβων. Χαρακτηριστικό παράδειγμα τέτοιων συσκευών αποτελούν οι αισθητήρες, οι οποίοι είναι τεχνολογία κομβική για την ανάπτυξης του IoT. Η διασύνδεση συσκευών μεταξύ τους και στο διαδίκτυο παρέχει τη δυνατότητα συλλογής τεράστιου όγκου δεδομένων για επεξεργασία και ανάλυση. Τα δεδομένα σε πολλές περιπτώσεις αποτελούν ευαίσθητες πληροφορίες των οποίων η διασφάλιση από κυβερνοεγκληματίες είναι υψίστης σημασίας. Οι PUFs όπως αναλύθηκε, αποτελούν πρωτότυπο μηχανισμό ασφαλείας μέσω υλικού, που χαρακτηρίζονται από απλή αρχιτεκτονική, με την ιδιότητα να καταναλώνουν ελάχιστη ενέργεια. Ωστόσο, η τεχνολογία PUF χαρακτηρίζεται από προβλήματα. Οι συμβατικές υλοποιήσεις PUFs παρουσιάζουν ευαισθησία σε ορισμένες επιθέσεις αποτελώντας πρόκληση σχετικά με την εφαρμογή τους σε συστήματα IoT. Επιπρόσθετα, πρόκληση για την εφαρμογή PUFs είναι ο περιορισμός σε πόρους του υλικού των ενσωματωμένων συσκευών στο IoT δημιουργώντας την ανάγκη ανάπτυξης «ελαφρύτερων» PUFs. (Halak, et al., 16-19 Oct. 2016)

4.1 LHPUF

Λύση στις αυξανόμενες απαιτήσεις ασφαλείας που δημιουργήθηκαν κατά την ραγδαία εξάπλωση του IoT θα μπορούσε να αποτελέσει η τεχνολογία των PUFs. Ωστόσο, δεν είναι άμεσα εφαρμόσιμη στα συστήματα IoT, λόγω των περιορισμένων πόρων των συσκευών. Το LHPUF συντελεί ειδικά σχεδιασμένο PUF, το οποίο είναι μία «ελαφριά» και ασφαλή τεχνολογία που ενδείκνυται για τους αυστηρούς περιορισμούς σε πόρους των συστημάτων IoT.

Το LHPUF χαρακτηρίζεται ως υβριδικό PUF. Ο χαρακτηρισμός αυτός πηγάζει από γεγονός ότι πρόκειται για συνδυασμό PUF Arbiter και RO. Αυτές οι δύο συμβατικές υλοποιήσεις PUFs παρουσιάζουν ευαισθησία σε επιθέσεις μηχανικής εκμάθησης και πλευρικών καναλιών. Η υβριδική τεχνολογία που χαρακτηρίζει το ειδικά σχεδιασμένο PUF παρέχει βελτιωμένη ασφάλεια και διακρίνεται από μικρότερη κατανάλωση ενέργειας. Άλλωστε, όπως έχει αναλυθεί, η απαίτηση σε ενέργεια των συσκευών του IoT είναι ιδιαίτερο χαρακτηριστικό έναντι των παραδοσιακών ψηφιακών συστημάτων. Επομένως, αυτές οι ειδικά σχεδιασμένες PUF ενδείκνυνται για τα συστήματα IoT.



Εικόνα 13: Δομή LHPUF[15].

Το LHPUF σε αντίθεση με τα συμβατικά PUF, πειραματικά επιτυγχάνει περισσότερη μοναδικότητα στις αποκρίσεις αποτελώντας βασικό δείκτη ποιότητας

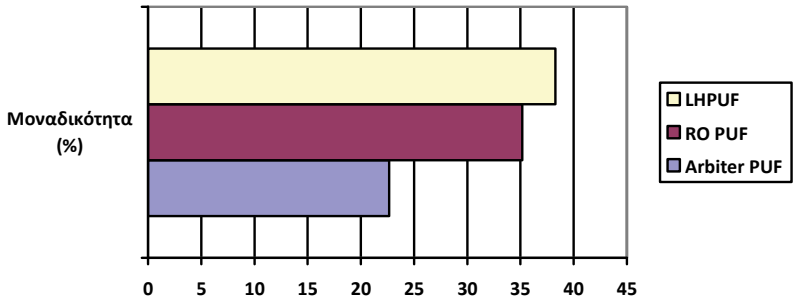
[15] https://ieeexplore.ieee.org/abstract/document/8719335

των PUFs. Χαρακτηριστικά, σε σύγκριση με το RO PUF επιτυγχάνει 3,1% περισσότερη μοναδικότητα και σε σύγκριση με το Arbiter PUF 15,1%. Τα ποσοστά αυτά αποδεικνύουν την αυξημένη ανθεκτικότητα σε επιθέσεις εισβολέων. Η περιοχή (αριθμός «φετών» που καταλαμβάνονται στο FPGA), η καθυστέρηση και η κατανάλωση ισχύος των υπαρχόντων PUF συνοψίζονται στον παρακάτω Πίνακα. Οι συμβατές PUFs βάσει καθυστέρησης συγκρίνονται με τα PUFs τεχνολογίας LHPUF. Σύμφωνα με τον Πίνακα, το LHPUF καταναλώνει λιγότερη ισχύ σε σύγκριση με τα υπάρχοντα PUFs με καθυστέρηση.

PUFs	Περιοχή	Καθυστέρηση	Κατανάλωση Ισχύος
Arbiter PUF	97	10.875	0.0081
XOR PUF	5	2.258	0.030
Feed Forward PUF	102	18.861	1.100
RO PUF	50	3.463	0.051
LHPUF	123	10.753	0.0025

Πίνακας 2: Ανάλυση PUFs[16].

Όπως έχει αναλυθεί στο κεφάλαιο 3 (υποενότητα 3.2.1 και 3.2.2), οι έξοδοι των RO PUF και Arbiter PUF είναι σε μεγάλο βαθμό τυχαίες. Αυτό αποδεικνύει έμμεσα την τυχαιότητα του προτεινόμενου LHPUF.



Γράφημα 2: Σύγκριση Μοναδικότητας LHPUF με συμβατικές υλοποιήσεις PUFs[17].

Η ειδικά σχεδιασμένη LHPUF απαρτίζεται από πολυπλέκτες, δύο μετρητές, συγκριτές, μία πύλη NAND, μία πύλη NOT, ένα κύκλωμα arbiter, δύο RO PUF και D flip flop. Η υβριδικότητα που χαρακτηρίζει το LHPUF αυξάνει κατά 4% τουλάχιστον το μέτρο της μοναδικότητας, καθώς διακρίνεται από αυξημένη πολυπλοκότητα σε

[16] https://ieeexplore.ieee.org/abstract/document/8719335
[17] https://ieeexplore.ieee.org/abstract/document/8719335

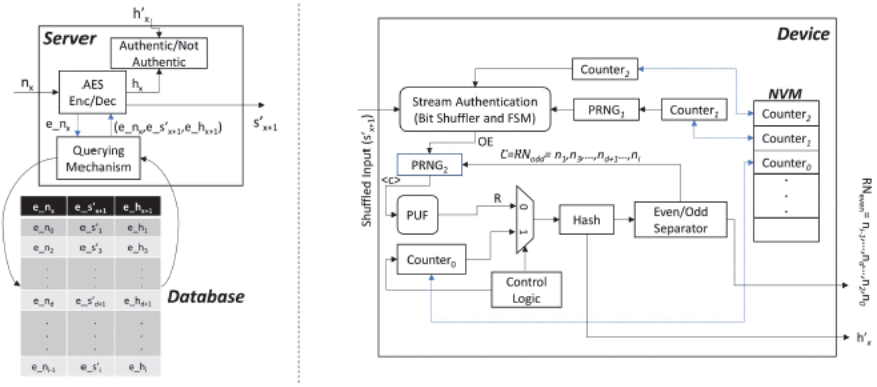
επίπεδο κυκλώματος γεγονός που δημιουργεί απρόβλεπτες αποκρίσεις. Επιπρόσθετα, το LHPUF καταναλώνει λιγότερη ισχύ και λιγότερη ενέργεια, συνεπώς το καθιστά κατάλληλο και αποτελεσματικό για την εφαρμογή του στο IoT [41]. (Sankaran, et al., 17-19 Dec. 2018).

4.2 PUF-IPA

Η χρήση των PUFs στο IoT αποτελεί λύση για την ασφαλή αναγνώριση των συσκευών αξιοποιώντας τα ιδιαίτερα χαρακτηριστικά υλικού των τσιπ των ολοκληρωμένων κυκλωμάτων. Όμως, τα συστήματα ελέγχου ταυτότητας που βασίζονται σε PUFs παρουσιάζουν ευαισθησία σε ορισμένες επιθέσεις. Οι επιθέσεις μοντελοποίησης και οι relay attacks δεν περιορίζονται από τις συμβατικές τεχνολογίες PUF.

Ειδικά σχεδιασμένη PUF για την βελτίωση των αποκρίσεων σε επιθέσεις που τείνουν να βλάψουν τα συστήματα IoT, αποτελεί το PUF-IPA. Παρά το γεγονός, ότι η τεχνολογία των PUFs παρέχει λύση για τον έλεγχο ταυτότητας, εμφανίζει τρωτότητα, όπως έχει αναλυθεί, σε επιθέσεις μοντελοποίησης που βασίζονται στην μηχανική εκμάθηση. Οι επιθέσεις αυτές δίνουν την δυνατότητα στο επιτιθέμενο άτομο να αναπαράγει τη συμπεριφορά των αποκρίσεων της συσκευής. Από το ζεύγος πρόκλησης-απόκρισης, ο εισβολέας μπορεί να δημιουργήσει ένα ακριβές μοντέλο πρόβλεψης.

Το PUF-IPA συγκροτεί μια ειδικά σχεδιασμένη τεχνολογία που χρησιμοποιεί PUFs για την παροχή ελέγχου ταυτότητας και την διατήρηση της ταυτότητας των συσκευών. Το PUF-IPA αποθηκεύει ασαφείς, μη συσχετισμένα δεδομένα που αφορούν το PUF της συσκευής στο διακομιστή και ο διακομιστής επικυρώνει τις συσκευές αυτές χρησιμοποιώντας τα δεδομένα χωρίς να έχει στην κατοχή του τα δεδομένα πρόκλησης απόκρισης. Αυτό έχει σαν αποτέλεσμα, ακόμη και εάν ο εισβολέας κατορθώσει να παραβιάσει τον διακομιστή και αποκτήσει πρόσβαση στα δεδομένα, δεν θα μπορεί να μοντελοποιήσει τις συσκευές μέσω μηχανικής μάθησης. Αυτό γιατί, οι προκλήσεις- αποκρίσεις που σχετίζονται με τα PUFs είναι γνωστές μόνο στη συσκευή.



Εικόνα 14: Διακομιστή μαζί με τη βάση δεδομένων και η πλευρά συσκευής[18].

Επιπρόσθετα, λόγω του καθημερινού εκθετικά αυξανόμενου αριθμού των συσκευών που συνδέονται στα IoT, η Αποθήκευση ζευγών προκλήσεων- αποκρίσεων θα είχε τεράστιο κόστος σε μνήμη, σε ισχύ και σε ενέργεια συνεπώς και χρηματικό. Το ειδικά σχεδιασμένο PUF-IPA για τα συστήματα IoT, παρέχει πιστοποίηση συσκευής χωρίς να αποθηκεύει CRP (ζεύγη) ή παρέχει ένα μοντέλο στη μνήμη του διακομιστή, όπου ο διακομιστής επικυρώνει τη συσκευή βασισμένος σε μη συσχετισμένα δεδομένα.

Όπως και στην περίπτωση του LHPUF, το PUF-IPA παρέχει έναν αποτελεσματικό και ελαφρύ μηχανισμό ελέγχου ταυτότητας συσκευής IoT. Το παραπάνω τεχνολογικό μοντέλο διακρίνεται από περιορισμένη κατανάλωση σε ισχύ, ως εκ τούτου ενδείκνυται στα πλαίσια της ασφάλειας του IoT.

Τεχνολογία που συνδυάζεται άμεσα με το PUF-IPA αποτελεί ο αλγόριθμος «ανακατέματος Fisher-Yates». Η ειδική PUF, έχει ενσωματωμένο αυτόν τον αλγόριθμο. Ο αλγόριθμος «ανακατέματος» σχετίζεται άμεσα με τον έλεγχο ταυτότητας. Το «ανακάτεμα» που πραγματοποιεί ο αλγόριθμος Fisher-Yates συντελείται κατά την εγγραφή μίας συσκευής. Στο μοντέλο αυτό χρησιμοποιείται και ένας μηχανισμός ελέγχου βασισμένος σε σημαίες. Ο μηχανισμός αυτός, παρέχει ένα επιπλέον επίπεδο ασφάλειας ενάντια σε εισβολείς οι οποίοι στοχεύουν να διεισδύσουν στη συσκευή με τυχαίες εισόδους. Κάθε φορά που αλλάζει η κατάσταση, η σημαία της κατάστασης αυξάνεται κατά ένα και παράλληλα αυξάνεται και το σήμα ενεργοποίησης εξόδου (OE). Εάν οι καταστάσεις έχουν την ίδια τιμή με τη ροή εισόδου, τότε υπάρχει εγκυρότητα. Στο PUF-IPA χρησιμοποιείται και ένας

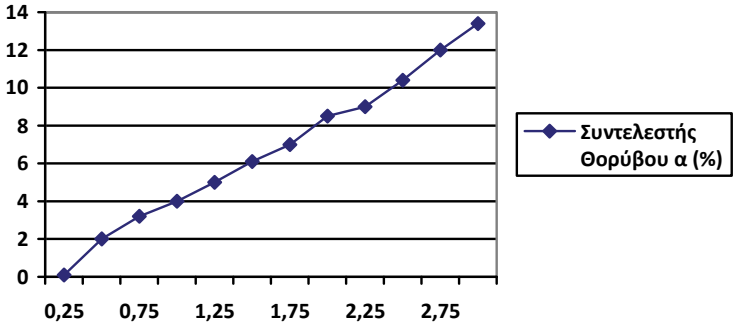
[18] https://ieeexplore.ieee.org/abstract/document/9045264

μηχανισμός κλειδώματος που βασίζεται σε FSM ο οποίος επιτρέπει στην συσκευή να παρακάμψει προσωρινά σφάλματα.

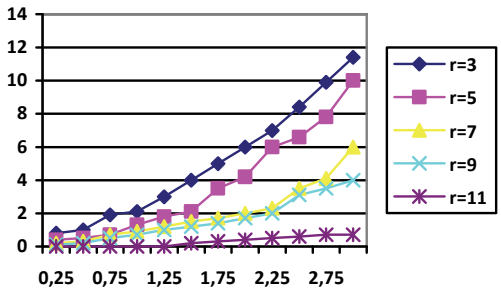
Σχεδιαστικά το PUF-IPA βασίζεται στην τεχνολογία Arbiter PUF για την παραγωγή αξιόπιστων αποκρίσεων και σε έναν αλγόριθμο κατακερματισμού των αποκρίσεων αυτών. Δεν αποθηκεύονται τα ζεύγη προκλήσεων-αποκρίσεων γεγονός που χαρακτηρίζει αυτά τα PUFs από αξιοπιστία. Έτσι, σε συνδυασμό με την έλλειψη ανάγκης πρόσθετης μνήμης, το PUF-IPA ενδείκνυται για την ενσωμάτωση τους σε συσκευές IoT. Για την αποτροπή επιθέσεων μοντελοποίησης μέσω μηχανικής εκμάθησης εφαρμόζεται σε αυτές τις ειδικά σχεδιασμένες PUFs μία ισχυρή λογική ελέγχου πρόσβασης. Προκειμένου να παράγει σταθερές αποκρίσεις εισάγεται ο μηχανισμός αυτοελέγχου. Αυτός ο μηχανισμός αξιολογεί επαναληπτικά την πρόκληση για κάποιο αριθμό, ο οποίος αποκαλείται παράγοντας αξιοπιστίας και το bit εξόδου της απόκρισης επιλέγεται βάση πλειοψηφίας που ψηφίζει με 0 ή 1. Η διαδικασία αυτή πραγματοποιείται σε κάθε απόκριση εξασφαλίζοντας την σταθερότητα.

Πλεονέκτημα του PUF-IPA φαίνεται να είναι το γεγονός ότι η συσκευή έχει τη δυνατότητα να εκτελεί δυναμικό έλεγχο αξιοπιστίας των προκλήσεων. Ο έλεγχος αυτός αποτρέπει τη χρήση προκλήσεων που παράγουν θορυβώδεις απαντήσεις λόγω περιβαλλοντικών επιπτώσεων, και κατά συνέπεια αποτελούν πιο αξιόπιστους μηχανισμούς άμυνας στο υλικό συγκριτικά με συμβατικές υλοποιήσεις PUFs, αφού βελτιώνουν την συμπεριφορά τους έναντι περιβαλλοντικών επιπτώσεων. Άλλο ένα πλεονέκτημα της τεχνολογίας PUF-IPA είναι ότι αντιμετωπίζουν relay επιθέσεις. Λόγω του μηχανισμού κλειδώματος που διαθέτει το PUF-IPA, η συσκευή θα κλειδωθεί μετά από συγκεκριμένο αριθμό προσπαθειών.

Στα παρακάτω γραφήματα παρουσιάζεται η μεγαλύτερη ακρίβεια απόκρισης του PUF-IPA έναντι προηγούμενων προτεινόμενων πρωτοκόλλων. Η ακρίβεια αυτή εκδηλώνεται από την δυνατότητα να εκτελεί το PUF-IPA δυναμικό έλεγχο αξιοπιστίας των προκλήσεων.



Γράφημα 3: Ακρίβεια απόκρισης έναντι διαφορετικών τιμών του α μιας μοναδικής παρουσίας PUF[19].



Γράφημα 4: Ακρίβεια απόκρισης για την ίδια παρουσία PUF με δυνατότητα αυτόματου ελέγχου[20].

Δεδομένου ότι η συσκευή έχει ρητό έλεγχο των δικών της προκλήσεων, έχει την δυνατότητα να ελέγξει αυτόνομα την ακρίβεια της απόκρισης χωρίς άδεια από το διακομιστή σε τυχαίες στιγμές. Υποθέτοντας ότι τη στιγμή tn, το περιττό δείκτη RN είναι nd + 1 και η συσκευή αξιολογεί το PUF με r = 11. Εάν οποιοδήποτε από τα bit απόκρισης έχει ποσοστό σφάλματος κοντά στο 40% (λόγος bit απόκρισης μειοψηφίας προς πλειοψηφία ≈ 4: 7), τότε αυτό το RN απορρίπτεται και δημιουργείται ένα νέο RN το οποίο θα χρησιμοποιηθεί για την διαδικασία ελέγχου ταυτότητας. Αυτό εξασφαλίζει συμβάντα ελέγχου ταυτότητας χωρίς θόρυβο ακόμη και κατά τη διάρκεια περιβαλλοντικών αλλαγών. Παρά το γεγονός ότι ο αυτοέλεγχος μπορεί να βελτιώσει δραστικά την ακρίβεια της απόκρισης, ο δυναμικός έλεγχος μπορεί να

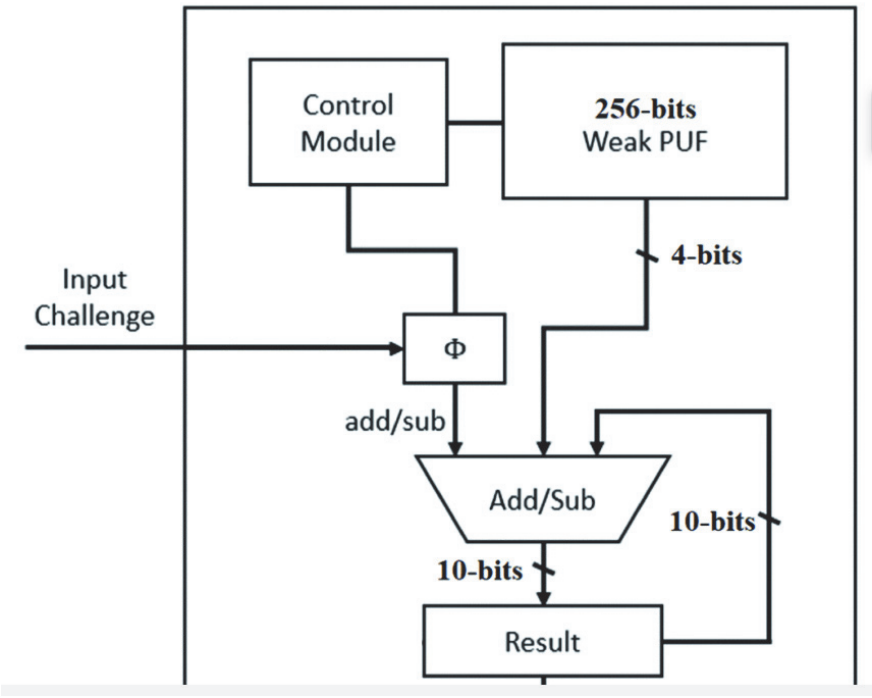
[19] https://ieeexplore.ieee.org/abstract/document/9045264
[20] https://ieeexplore.ieee.org/abstract/document/9045264

αποτρέψει τη χρήση προκλήσεων που προκαλούν θορυβώδεις απαντήσεις λόγω περιβαλλοντικών επιπτώσεων κατά τη διάρκεια συμβάντων ελέγχου ταυτότητας.

Συνοψίζοντας, το PUF-IPA ενδείκνυται στα πλαίσια της ασφάλειας για το IoT, καθώς είναι ελαφρύ και επεκτάσιμο. Ερευνητές έχουν αποδείξει ότι αυτή η τεχνολογία είναι αξιόπιστη και μπορεί να συμβάλει την διατήρηση του απορρήτου, προστατεύοντας την πρόσβαση στα δεδομένα από κακόβουλα άτομα. Τέλος, το PUF-IPA διατηρεί την ταυτότητα των συσκευών χωρίς να επιβαρύνει την μνήμη του διακομιστή, έτσι αυτό αποτελεί άλλο ένα κίνητρο για την χρήση τους σε συσκευές του IoT, όπου οι μνήμες είναι περιορισμένες [40]. (Qureshi, et al., 10-13 Jan. 2020).

4.3 PUF ΒΑΣΙΣΜΕΝΕΣ ΣΤΗΝ ΜΝΗΜΗ

Τα PUF βασισμένα στην μνήμη (Mem APUF) αξιοποιούν χαρακτηριστικά της μνήμης στο υλικό για την προστασία των συστημάτων του IoT. Αναλυτικότερα, τα συγκεκριμένα PUFs χρησιμοποιούν τα τσιπ μνήμης των συσκευών για την «θωράκιση του IoT» έναντι επιθέσεων. Η παραπάνω τεχνολογία PUF βασίζεται σε διάφορους τύπους μνήμης, όπως SRAM, MRAM, Flash και memristor. Σε αντίθεση με τις συμβατικές υλοποιήσεις PUFs, απαιτούν ελάχιστο ή καθόλου πρόσθετο υλικό. Αυτό αποτελεί πλεονέκτημα και δίνει σαφές προβάδισμα στην χρήση τέτοιων PUFs ως μηχανισμό ασφαλείας στο IoT, αφού οι συσκευές του συστήματος IoT χαρακτηρίζονται από περιορισμένο μέγεθος και ισχύ σε αντίθεση με τα παραδοσιακά ψηφιακά συστήματα. Το γεγονός ότι απαιτούν ελάχιστο πρόσθετο υλικό συνεπάγεται μικρότερη κατανάλωση ενέργειας, κάτι το οποίο εναρμονίζεται με τις κατασκευαστικές απαιτήσεις των συσκευών του IoT.

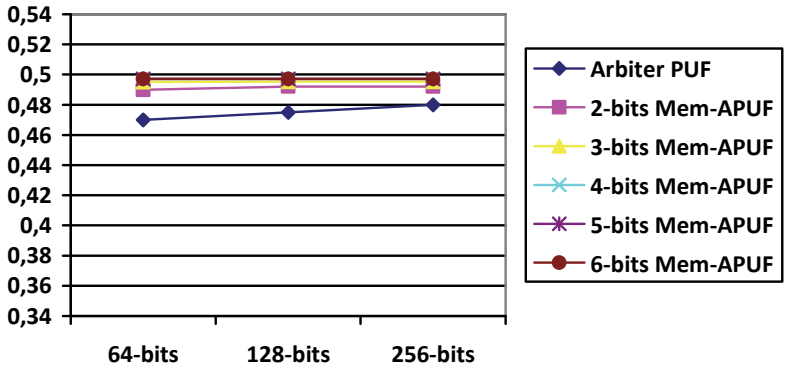


Εικόνα 15: Αρχιτεκτονική PUFs βασισμένα στην μνήμη[21].

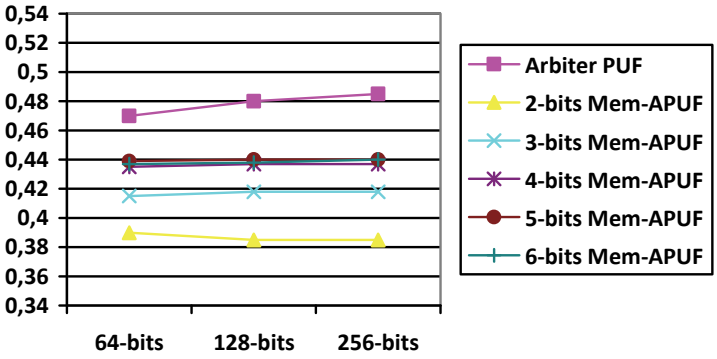
Τα Mem APUFs προσφέρουν σύντομο χρόνο υπολογισμού. Το computing αποτελεί ιδιαιτερότητα του IoT σε αντίθεση με το παραδοσιακό υλικό. Οι ειδικά σχεδιασμένες PUFs απαιτούν πυκνότητα 128 με 256 bit για την δημιουργία κλειδιών στα πλαίσια της επικοινωνίας για την ασφάλεια των δεδομένων, η οποία είναι μικρή συγκριτικά με την μνήμη των συσκευών στο IoT. Έτσι, η χρήση της τεχνολογίας αυτής αυξάνει την ασφάλεια των συσκευών του IoT, καθώς ελάχιστο ποσοστό μνήμης θα χρησιμοποιηθεί για την δημιουργία κλειδιών και έτσι δυσκολεύει το έργο των επιτιθέμενων να εντοπίσουν το τμήμα μνήμης των κλειδιών. Κατα αυτό το γεγονός, καθιστά την υλοποίηση PUF αυτή, καλό αντίμετρο σε Hardware Trojan επιθέσεις.

Στην παρακάτω γραφική αναπαράσταση παρουσιάζεται η τυχαιότητα και η μοναδικότητα του PUF σε ποικίλο πλάτος bit ενός Mem-APUF σε σύγκριση με αυτό ενός Arbiter PUF (υποενότητα 3.2.2). Μετράται σε διάφορα μήκη bit PUF: 64, 128 και 256 μεγεθών εισόδου.

[21] https://ieeexplore.ieee.org/abstract/document/9221015



Γράφημα 5: Η τυχαιότητα του PUF σε ποικίλο πλάτος bit ενός Mem- Arbiter PUF σε σύγκριση με αυτό ενός Arbiter PUF[22].



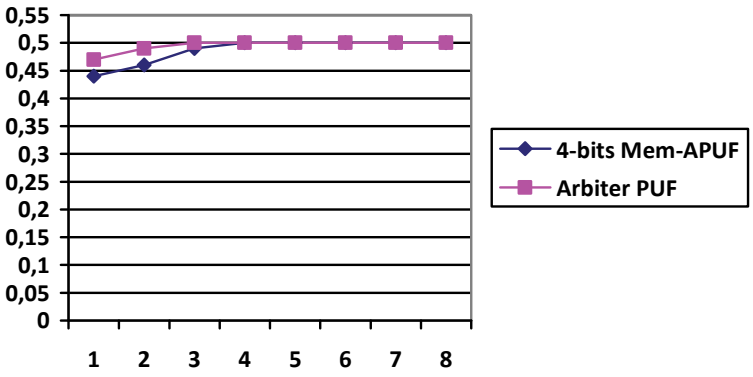
Γράφημα 6: Η μοναδικότητα του PUF σε ποικίλο πλάτος bit ενός Mem-APUF σε σύγκριση με αυτό ενός Arbiter PUF[23].

Ο συνδυασμός αυτής της τεχνολογίας με τα προηγμένα πρωτόκολλα που επιτρέπουν την αλλαγή κελιών μνήμης από τα οποία εξαρτάται η απόκριση, αυξάνουν την ασφάλεια, καθώς κάθε φορά χρησιμοποιείται διαφορετικό κλειδί για τον έλεγχο ταυτότητας. Τα PUFs που βασίζονται στην μνήμη μπορούν να θωρακίσουν τα συστήματα IoT, προσφέροντας έλεγχο ταυτότητας και ακόμη την δυνατότητα εξαγωγής των ιδιωτικών κρυπτογραφικών κλειδιών από την μνήμη των συσκευών χωρίς την αύξηση επιπλέον χρηματικού κόστους. Το οικονομικό κόστος είναι ιδιαίτερο χαρακτηριστικό των συσκευών IoT σε σχέση με τις παραδοσιακές

[22] https://ieeexplore.ieee.org/abstract/document/9221015
[23] https://ieeexplore.ieee.org/abstract/document/9221015

συσκευές, διότι οι συσκευές του IoT οφείλουν να χαρακτηρίζονται από μικρό κόστος [44]. (Akinaga, et al., 2010).

Στα παρακάτω σχήματα θα παρουσιαστεί η διαφορά στις τιμές μοναδικότητας ενός 4-bit XOR Mem-APUF[24] και του παραδοσιακού Arbiter PUF.



Γράφημα 7: Επίδραση του XORing πολλαπλών PUF στη μοναδικότητα όταν χρησιμοποιούνται Mem-APUF 4-bit και Arbiter PUF[25].

Όπως διακρίνεται η διαφορά στις τιμές μοναδικότητας ενός 4-bit XOR Mem-APUF και του παραδοσιακού Arbiter PUF, καθίσταται αμελητέα πέρα από τις 3 εξόδους XOR. Καθώς το Mem-APUF προορίζεται να αυξήσει την ασφάλειά του χρησιμοποιώντας κυρίως XOR-ing ή άλλες τεχνικές όπως Feed-Forward APUFs ή LS PUF, η επιτευχθείσα μοναδικότητα με 4 bit θα ήταν περισσότερο από επαρκής.

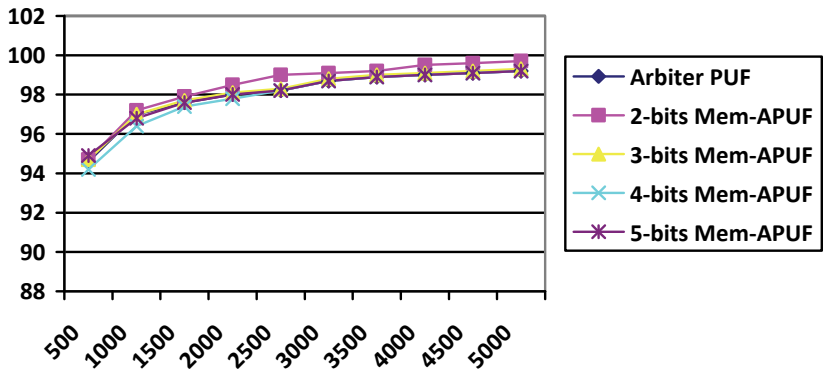
Η αντίσταση ενός PUF σε επιθέσεις μοντελοποίησης αποτελούν ιδιαίτερα σημαντικό παράγοντα πίσω από την ασφάλεια του PUF. Αυτή η αντίσταση μετριέται σε NCR[26]. Συγκρίνουμε την ακρίβεια πρόβλεψης μιας επίθεσης με βάση το Linear Regression στο Mem-APUF (PUF βασισμένο στην μνήμη) με τιμές μήκους από 2 έως 5 bit καθώς και το παραδοσιακό APUF. Η ακρίβεια της πρόβλεψης που επιτεύχθηκε μοιάζει σε μεγάλο βαθμό με την εξαίρεση του 2-bit που έδειξε αυξημένη ευπάθεια στην επίθεση. Ως αποτέλεσμα, οποιαδήποτε τιμή μεγαλύτερη ή ίση με 3 bits για μήκος μεμονωμένων ωρών καθυστέρησης θα διασφαλίσει ότι το Mem-APUF θα ταιριάζει με την αρχική ασφάλεια Arbiter PUF.

[24] Memory Arbiter PUF
[25] https://ieeexplore.ieee.org/abstract/document/9221015
[26] Ο αριθμός των αυθεντικών ζευγών πρόκλησης-απόκρισης που πρέπει να παρατηρηθεί από έναν επιτιθέμενο προκειμένου να επιτευχθεί μια συγκεκριμένη ακρίβεια πρόβλεψης.

Η ασφάλεια Arbiter PUF αυξάνεται συχνά με χρήση XOR-ing, προώθησης τροφοδοσίας ή άλλων τύπων κυκλωμάτων όπως το Lightweight Secure PUF[27] (LS PUF). Σημαντικός παράγοντας είναι να διασφαλιστεί ότι το εισαγόμενο Mem-APUF μπορεί να κλιμακωθεί με παρόμοιο τρόπο. Για να προσδιοριστεί ένα μήκος bit για τα βάρη που μπορούν να διασφαλίσουν τέτοια ανάπτυξη, εφαρμόζεται ένα κλιμακωτό κύκλωμα Mem-APUF με XOR-έξοδο από τρεις παρουσίες της μονάδας. Πάνω σε αυτό, πραγματοποιούνται επιθέσεις μοντελοποίησης χρησιμοποιώντας νευρωνικά δίκτυα. Τα αποτελέσματα συγκρίνονται με παρόμοιες επιθέσεις που πραγματοποιήθηκαν σε APUF 3-XOR. Από τον παρακάτω Πίνακα, συνεπάγεται ότι επιλέγοντας ένα πλάτος bit 4 bit για τα βάρη μπορεί να διασφαλιστεί συγκρίσιμη κλίμακα ασφαλείας με αυτό ενός παραδοσιακού Arbiter PUF.

	3-bits Mem-APUF	**4-bits Mem-APUF**	**5-bits Mem-APUF**	**Arbiter PUF**
3 XORs	(10k,13.5k)	(20k,45k)	(18k,44 k)	(22k,45k)

Πίνακας 3: Ο αριθμός των CRP που πρέπει να φτάσει σε ακρίβεια πρόβλεψης 95% και 99% για διαφορετικό πλάτος bit Mem-APUF μαζί με το APUF[28].



Γράφημα 8: Αριθμός CRPs έναντι ακρίβειας πρόβλεψης για ποικίλα σχέδια Mem-APUF σε σύγκριση με Arbiter PUF.

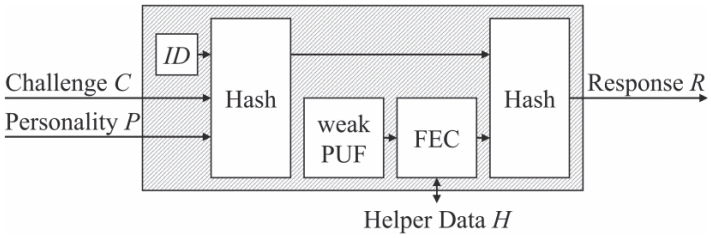
[27] Ο σχεδιασμός τους περιλαμβάνει ένα δίκτυο εισόδου που αναδιατάσσει και αλλάζει τον τρόπο τροφοδοσίας των εισόδων πρόκλησης εξασφαλίζοντας αυξημένη απόσταση Hamming για τις εισόδους. . Επιπρόσθετα, περιλαμβάνεται ένα δίκτυο εξόδου με XOR και πολλές τιμές arbiter, χρησιμοποιώντας τους ίδιους διαιτητές σε πολλά XORs αυξάνοντας την απόδοση του σχεδιασμού.

[28] https://ieeexplore.ieee.org/abstract/document/9221015

Ενώ η τιμή των 3 bits για το μήκος των βαρών θα αρκούσε για ασφάλεια, η δοκιμή μοναδικότητας έδειξε ότι τα 4-bits θα προσφέρουν καλύτερη τιμή μοναδικότητας και είναι το κατώφλι πριν από τη μείωση των επιστροφών προσφέρουν μικρό κέρδος στην αύξηση του μήκους bit. Έτσι, μια τιμή 4 bit για το μήκος των βαρών φαίνεται να είναι η βέλτιστη επιλογή σχετικά με όλες τις μετρήσεις: ασφάλεια, τυχαιότητα και μοναδικότητα.

4.4 C-PUF

Η επίθεση ‘‘man-in-the-middle’’ αποτελεί μία δημοφιλή απειλή στα συστήματα IoT. Στην επίθεση αυτή ο εισβολέας εκμεταλλεύεται την ευπάθεια σε επίπεδο μετάδοσης δεδομένων των ασύρματων αισθητήρων. Τα δεδομένα και οι πληροφορίες είναι ευαίσθητες παράμετροι, στα οποία εάν ο κακόβουλος καταφέρει να αποκτήσει πρόσβαση το αντίκτυπο θα είναι μεγάλο. Ερευνητές ανέδειξαν ελεγχόμενα PUFs γνωστά ως Controller PUF (C-PUF). Τα C-PUF μπορούν να διαχειριστούν επιθέσεις κατασκοπίας man in the middle (ελληνικά: Άνθρωπος στην Μέση).



Εικόνα 16: Δομή ελεγχόμενου PUF με ασθενές PUF και κώδικα διόρθωσης σφαλμάτων προς τα εμπρός (FEC)[29].

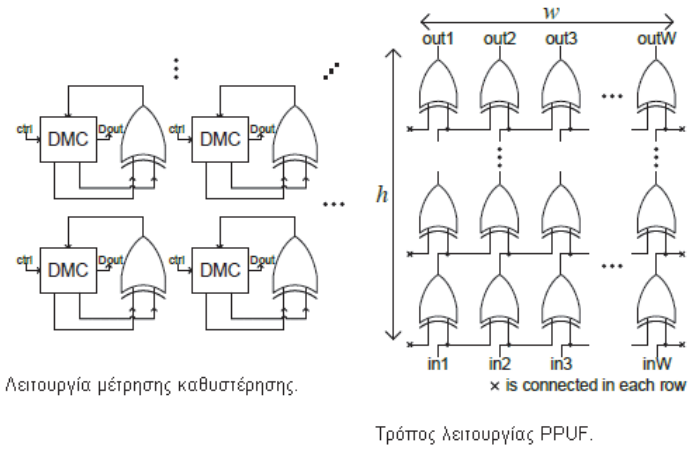
Ο συγκεκριμένος τύπος PUF χρησιμοποιεί έναν συγκεκριμένο αλγόριθμο. Η πρόσβαση στις πληροφορίες γίνεται μόνο με χρήση του συγκεκριμένου αλγορίθμου. Ο αλγόριθμος λειτουργεί με μία συνάρτηση κατακερματισμού, η οποία είναι

[29] https://ieeexplore.ieee.org/abstract/document/7457156

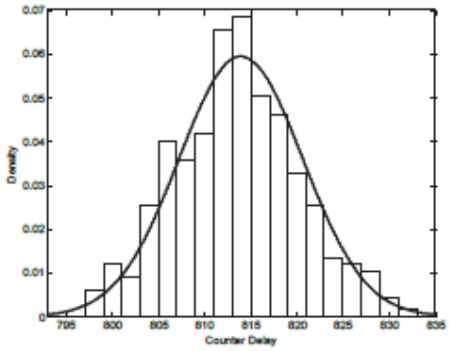
ανθεκτική έναντι συγκρούσεων. Επίσης, σε αυτό το τύπο PUF τοποθετείται ένας κωδικός διόρθωσης σφάλματος μετά την απόκριση επιτυγχάνοντας τη μείωση των θορύβων των μετρήσεων της εξόδου, έχοντας ως αποτέλεσμα, οι έξοδοι (αποκρίσεις) των PUF αυτών να ισχυροποιούνται. Έτσι, το PUF δεν παρουσιάζει σε τέτοιες επιθέσεις τρωτότητα, άρα έχει προβάδισμα έναντι συμβατών PUF. Η πρόσβαση σε αυτές τις ειδικά σχεδιασμένες PUF μπορεί να πραγματοποιηθεί μόνο από έναν αλγόριθμο που συνδέεται φυσικά με το PUF. Η ενσωμάτωση του συγκεκριμένου τύπου PUF στα συστήματα IoT αποτελεί αντικείμενο συνεχούς μελέτης από την επιστημονική κοινότητα [42,43]. (B. Gassend, et al., 2002) (Tehranipoor, et al., 2011)

4.5 PUBLIC-PUF

Ειδικά σχεδιασμένη PUF αποτελεί η Public PUF (PPUF). Αυτή η νέα κατηγορία PUF συγκροτεί ένα καλό αντίμετρο σε επιθέσεις πλευρικών καναλιών, που παρουσιάζουν ευαισθησία PUF. Η PPUF χαρακτηρίζεται από ένα ορθογώνιο κύκλωμα κατασκευασμένο από πύλες XOR. Οι αποκρίσεις αυτού του τύπου PUF εξαρτώνται από τις καθυστερήσεις των πυλών. Για την προσομοίωση των αποκρίσεων χρειάζεται αρκετός χρόνος γεγονός που λειτουργεί κατασταλτικά σε επιθέσεις κακόβουλων ατόμων. Το PPUF πρέπει να φτάσει στο σημείο σταθερής κατάστασης προτού την προσομοίωση λόγω των καθυστερήσεων των ενδιάμεσων πυλών. Αυτό το γεγονός έχει σαν αποτέλεσμα, να προστίθεται στον χρόνο προσομοίωσης και χρόνος σταθεροποίησης της κατάστασης του κυκλώματος [54]. (Beckmann, et al., 2009).



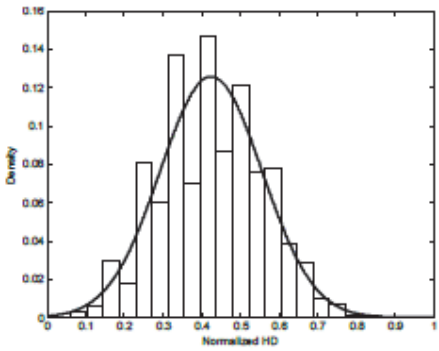
Εικόνα 17: Αρχιτεκτονική υλικού PPUF[30].



Γράφημα 9: Μετρήσεις καθυστέρησης πύλης[31].

Στο παραπάνω γράφημα, επιτυγχάνεται η αξιολόγηση της απόδοσης του υλικού των δακτυλικών αποτυπωμάτων PPUF σε σχέση με τη διανομή καθυστέρησης πύλης και τη μοναδικότητα. Οι μετρήσεις περιλαμβάνουν τις καθυστερήσεις για 336 πύλες σε κανονική θερμοκρασία λειτουργίας από μια πλακέτα FPGA. Στη παραπάνω γραφική αναπαράσταση, η τιμή μετρητή καθυστέρησης κυμαίνεται με μέση τιμή 813.9 και τυπική απόκλιση 6,7, όπου ένας μετρητής είναι περίπου 2,5 ns.

[30] https://ieeexplore.ieee.org/abstract/document/8057146
[31] https://ieeexplore.ieee.org/



Γράφημα 10: Κατανομή των μετρήσεων HD από board σε board σε κανονική θερμοκρασία λειτουργίας[32].

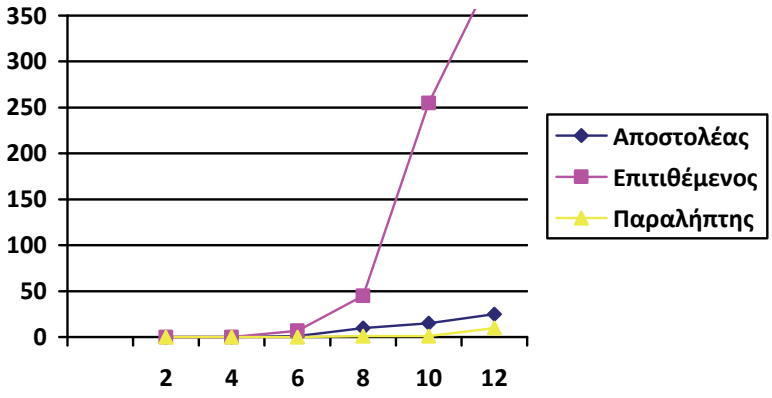
Στο γράφημα 10, παρουσιάζεται η κατανομή των μετρήσεων HD από board σε board σε κανονική θερμοκρασία λειτουργίας. Η απόσταση Hamming από πλακέτα σε πίνακα (HD) χρησιμοποιείται ως μέτρο μοναδικότητας, αντικατοπτρίζοντας το ποσοστό των bit απόκρισης που διαφέρουν μεταξύ δύο πλακέτων FPGA για μια δεδομένη κοινή πρόκληση. Η διαδικασία επαναλαμβάνεται με χίλια διαφορετικά σύνολα πρόκλησης. Η μέση τιμή του κανονικοποιημένου HD είναι 0,425, που είναι κοντά στο 0,5 (ιδανική τιμή). Ως εκ τούτου, η εφαρμογή PPUF FPGA ενσωματώνει διακριτική μεταβλητότητα ώστε να διακρίνει μεταξύ δύο διαφορετικών μονάδων ασφαλείας υλικού PPUF.

Η ανθεκτικότητα έναντι επιθέσεων πλευρικού καναλιού των ειδικά σχεδιασμένων PUF (PPUF), μπορεί να γίνει εύκολα κατανοητή εάν συλλογιστεί κανείς ότι έστω ένας επιτιθέμενος έχει στην διάθεση του CPU 10 GHz και με δεδομένο ότι η προσομοίωση ενός αριθμού στο PPUF απαιτεί πολλούς κύκλους για την υποκλοπή του κρυπτογραφικού κλειδιού. Έστω, ότι ο επιτιθέμενος έχει δύο δισεκατομμύρια υπολογιστές με ισχύ 10 GHz ανά ηλεκτρονικό υπολογιστή. Με την χρήση του PPUF ο συνολικός απαιτούμενος χρόνος είναι διακόσια ενενήντα τέσσερα χρόνια, δηλώνοντας ότι η απόκριση απαιτεί πολύ χρόνο. Αυτό έχει σαν αποτέλεσμα η συγκεκριμένη προσέγγιση PUF να χαρακτηρίζεται ανθεκτική σε επιθέσεις, που εκμεταλλεύονται φυσικές συμπεριφορές του υλικού των συσκευών, όπως την κατανάλωση ενέργειας, τιμές χρονισμού κ.α. προδίδοντας ευαίσθητες πληροφορίες [43]. (Helfmeier, et al., 2014)

[32] https://ieeexplore.ieee.org/abstract/document/8057146

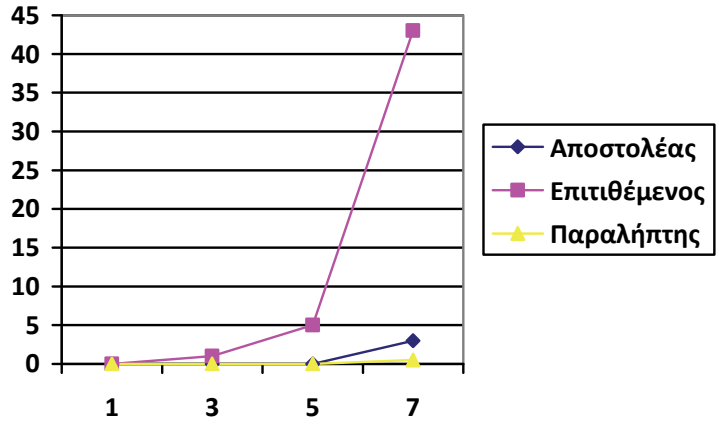
Παρακάτω θα αναπαρασταθεί γραφικώς η σύγκριση απόδοσης εκτέλεσης ελέγχου ταυτότητας στον αποστολέα, του προοριζόμενου παραλήπτη και του εισβολέα. Πειραματικώς, χρησιμοποιήθηκαν οι παράμετροι w = 8, h = 7 και m = 16 στο υλικό και λογισμικό PPUF. Στόχο τον μετρήσεων αποτελεί η έρευνα της πολυπλοκότητας του χρόνου εκτέλεσης. Όπου w, είναι το πλάτος του PPUF. Όσο το πλάτος αυξάνεται ο εισβολέας έχει έναν εκθετικά αυξανόμενο χρόνο εκτέλεσης. Σε ένα Raspberry Pi 2 board, ο επιτιθέμενος απέτυχε να ολοκληρώσει την προσομοίωση που θα κατάφερνε να ανακτούσε το μυστικό κλειδί πέραν του w = 10. Ο παραλήπτης χαρακτηρίζεται από δικό του υλικό και λογισμικό δακτυλικών αποτυπωμάτων PPUF. Σε αντίθεση με τον αποστολέας, ο παραλήπτης δαπανά ελαφρώς λιγότερο χρόνο για να ανακτήσει το μυστικό κλειδί. Το χρονικό κενό προκύπτει από το εάν η δημιουργία μυστικών κλειδιών πραγματοποιείται από υλικό δακτυλικών αποτυπωμάτων ή από καθαρό λογισμικό. Όπου h, είναι το ύψος του PPUF. Σχετικά με την επίδραση του h, ο μετρούμενος χρόνος εκτέλεσης δείχνει μια παρόμοια τάση με ποικίλο w όπως φαίνεται στο Γράφημα 11.

Έστω ότι οι παράμετροι της κλίμακας υλοποίησης PPUF χαρακτηρίζονται από τις τιμές 7 × 24 (όπου h = 7 και w = 24). Αποδεικνύεται ότι η αύξηση του w είναι ένας πολύ αποτελεσματικός τρόπος προστασίας από μια επίθεση brute-force, τιμωρώντας σοβαρά τον χρόνο εκτέλεσης της προσομοίωσης.



Γράφημα 11: Χρόνος εκτέλεσης με w(h=7,m=16)[33].

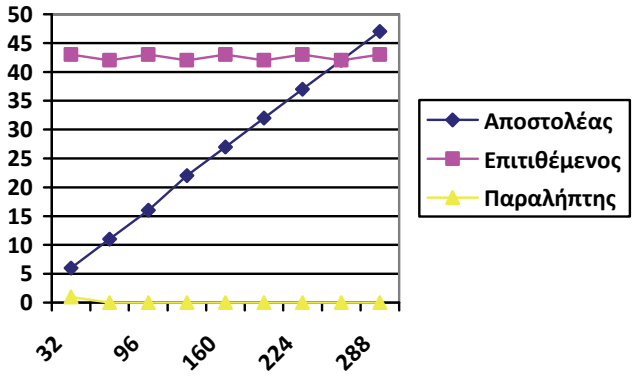
[33] https://ieeexplore.ieee.org/abstract/document/8057146



Γράφημα 12: Χρόνος εκτέλεσης με h(w=8,m=16)[34].

Σε αυτό το σημείο, διερευνάται το αποτέλεσμα του μήκους συνένωσης m. Η πολυπλοκότητα υπολογισμού επηρεάζεται σε μεγάλο βαθμό από το m για τον αποστολέα, τον επιτιθέμενο και τον παραλήπτη, Ο δέκτης και ο εισβολέας έχουν πραγματοποιήσει την εκτέλεση τους ανεξάρτητα από το μήκος συνένωσης m, ενώ ο χρόνος εκτέλεσης στον αποστολέα αυξάνεται γραμμικώς. Κατα αυτό το γεγονός, αποδεικνύεται ότι μπορεί να υπάρχει μια μέγιστη επιτρεπόμενη τιμή m όπου ο χρόνος εκτέλεσης του αποστολέα είναι ακόμη μεγαλύτερος από τον χρόνο του επιτιθέμενου. Έτσι, η αύξηση του μήκους της συνένωσης για τη βελτίωση της ασφάλειας κρυπτογράφησης μπορεί να βλάψει τη δημιουργία του προηγούμενου κλειδιού στον αποστολέα, οδηγώντας σε υψηλή κατανάλωση υπολογιστικών πόρων. Είναι σημαντική η κατάλληλη επιλογή παραμέτρων σχεδίασης των w, h και m για την εφαρμογή σε ένα σύστημα PPUF με υψηλή απόδοση και ασφάλεια λαμβάνοντας υπόψη τη σχετική σχέση απόδοσης.

[34] https://ieeexplore.ieee.org/abstract/document/8057146



Γράφημα 13: Χρόνος εκτέλεσης με m(w=8,h=7)[35].

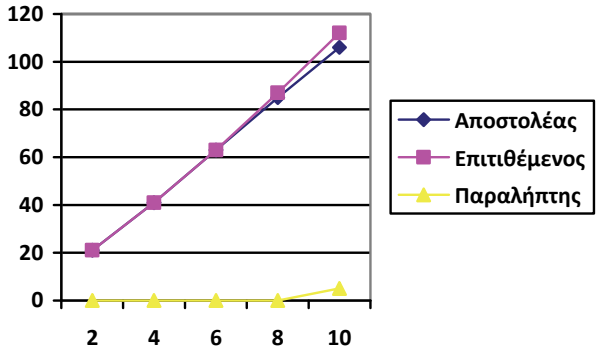
Όπως έχει αναλυθεί στο κεφάλαιο 2 (υποενότητα 2.2.2), το βασικός περιορισμός των συσκευών IoT καθιστά ο περιορισμός σε μνήμη και πόρους. Η κατανάλωση σε πόρους μνήμης των συστημάτων PPUF εξαρτάται άμεσα από τις παραμέτρους σχεδίασης των w και h. Όσο αυξάνεται το πλάτος w, τόσο ο αποστολέας όσο και ο επιτιθέμενος απαιτούν γραμμική αύξηση πόρων μνήμης, ενώ ο παραλήπτης χρησιμοποιεί σχετικά πολύ μικρή μνήμη. Καθώς το ύψος h αυξάνεται, τόσο ο αποστολέας όσο και ο επιτιθέμενος καταναλώνουν εκθετικά αυξανόμενη μνήμη, ενώ η χρήση μνήμης στον παραλήπτη είναι σχεδόν σταθερή, ανεξαρτήτως της τιμής του ύψους. Δηλαδή, ο αποστολέας και ο επιτιθέμενος χρειάζονται μεγάλο χώρο μνήμης για τη διατήρηση όλων των πιθανών μεταβάσεων, ενώ ο παραλήπτης έχει την δυνατότητα να καταγράψει μόνο κάθε είσοδο και την αντίστοιχη έξοδο εκτελώντας τη μονάδα υλικού PPUF.

Οι επιθέσεις brute-force πρακτικά ανέφικτες από την άποψη της πολυπλοκότητας αποθήκευσης και υπολογισμού. Η τεχνολογία PPUF μπορεί εύκολα να αποτελέσει μέτρο άμυνας σε επιθέσεις τέτοιες. Αυτό γιατί, υπάρχει η δυνατότητα να μεταφερθεί στον επιτιθέμενο υψηλό φορτίο ανάγκης σε μνήμη. Για να είναι αυτό δυνατό πρέπει απλώς να αυξηθεί το ύψος h είτε το πλάτος w του PPUF. Όμως,, αυτή η προσέγγιση υποβαθμίζει την απόδοση από την πλευρά του αποστολέα, καταστρέφοντας το ίδιο το σενάριο εφαρμογής. Από την άποψη της πολυπλοκότητας του υπολογισμού, από την άλλη πλευρά, η επιλογή μεγάλου w ή h μπορεί να είναι ένας τρόπος να κάνει έναν επιτιθέμενο να εκτελέσει την προσομοίωσή του με ένα

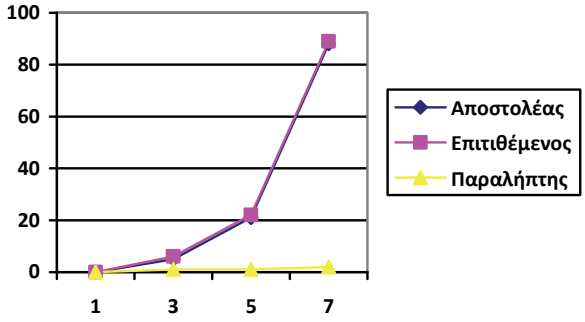
[35] https://ieeexplore.ieee.org/abstract/document/8057146

τεράστιο χρονικό διάστημα. Έτσι, είναι κρίσιμη η επιλογή ενός συγκεκριμένου εύρους τιμών w και h ώστε να καταστούν αδύνατη την επίθεση brute-force από πλευράς επιτιθέμενων, χωρίς να δαπανώνται πολλοί πόροι μνήμης από πλευράς αποστολέα.

Ακολουθούν τα γραφήματα μέτρησης αποτυπώματος μνήμης σε αποστολέα, του προοριζόμενου παραλήπτη και του εισβολέα:



Γράφημα 14: Χρήση μνήμης με w(h=7,m=16)[36].

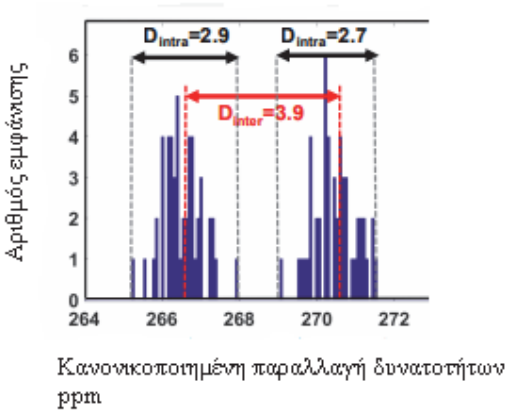


Γράφημα 15: Χρήση μνήμης με h (w=8,m=16)[37].

[36] https://ieeexplore.ieee.org/abstract/document/8057146
[37] https://ieeexplore.ieee.org/abstract/document/8057146

4.6 RADIO FREQUENCY PUF

Η χρήση της τεχνολογίας των PUFs αποτελεί αμυντικός μηχανισμός χαμηλού κόστους και «ελαφριά» από άποψη ισχύος για τα συστήματα IoT. Τα PUFs παρέχουν μηχανισμούς ελέγχου ταυτότητας και κρυπτογράφησης εκμεταλλευόμενα την κατασκευή τους. Ωστόσο, όπως έχει αναλυθεί, παρουσιάζουν ευαισθησία σε ορισμένες επιθέσεις διαταράσσοντας το απόρρητο αναφορικά με τα δεδομένα. Ειδικά σχεδιασμένη τεχνολογία PUF αποτελεί το RF-PUF, το οποίο εκμεταλλεύεται τις παραλλαγές των ραδιοσυχνοτήτων (RF) και την διαδικασία της μηχανικής μάθησης πετυχαίνοντας καλύτερες τιμές μοναδικότητας[38] και αξιοπιστίας[39].



Γράφημα 16: Μοναδικότητα και Αξιοπιστία[40].

Το παραπάνω γράφημα παρουσιάζει την αξιοπιστία και τη μοναδικότητα του RF-PUF. Η τεχνολογία RF-PUF ενσωματώνει εγγενώς τη μοναδική υπογραφή του δέκτη. Ως εκ τούτου, οι αποστάσεις Hamming Inter-PUF (μοναδικότητα) και Intra-PUF μπορούν να απεικονιστούν χρησιμοποιώντας τα κανονικοποιημένα μέρη ανα εκατομμύριο (ppm) παραλλαγή των χαρακτηριστικών εισαγωγής. Ωστόσο, απαιτείται

[38] Απόσταση Hamming Intra-PUF
[39] Απόσταση Inter-PUF Hamming
[40] https://arxiv.org/ftp/arxiv/papers/1805/1805.01048

ένας μετασχηματισμός των χαρακτηριστικών ώστε να αντιπροσωπεύουν τις παραλλαγές ppm σε έναν άξονα.

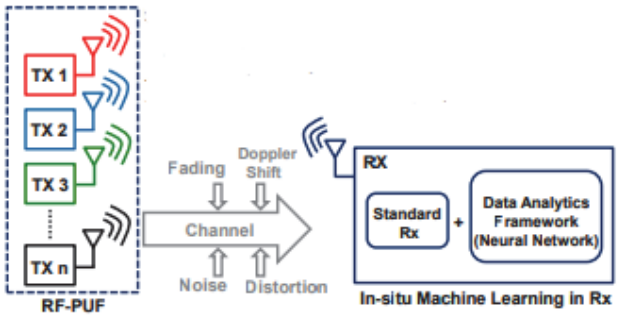
Από το παραπάνω διάγραμμα, η χειρότερη περίπτωση παραλλαγής μεταξύ PUF για 1000 πομπούς 3,9 ppm, ενώ η αντίστοιχη παραλλαγή εντός PUF είναι 2,9 ppm. Έτσι, παρά την μοναδικότητα που παρουσιάζεται για 1000 πομπούς, η πιθανότητα εσφαλμένης ανίχνευσης εξακολουθεί αυξάνεται καθώς ο αριθμός των πομπών φτάνει μερικές χιλιάδες. Η διαφορά μεταξύ της απόστασης Hamming μεταξύ PUF και εντός του PUF όπως παρουσιάζεται στο παραπάνω διάγραμμα μειώνεται [76,77,79]. (Sen, et al., 2008) (Banerjee, et al., 2014) (Suh, et al., 2007).

Η τεχνολογία αυτή δεν απαιτεί πρόσθετο υλικό και επιτρέπει την ασφαλή επικοινωνία σε ένα δίκτυο. Η λειτουργία του RF-PUF σε αντίθεση με παραδοσιακά PUF, εμφανίζει μεγαλύτερη ανθεκτικότητα απέναντι σε επιθέσεις πλευρικού καναλιού (side channel attack), μηχανικής μάθησης, επεμβατικές και ημι-επεμβατικές επιθέσεις οι οποίες επιβαρύνουν την μνήμη και την ισχύ των συσκευών [74,75]. (Maes, 2012) (Chatterjee, et al., 2018)

Για την διαδικασία της αναγνώρισης-ταυτοποίησης των συσκευών, το RF-PUF εκμεταλλεύεται την λειτουργία των PUFs σε συνδυασμό με έναν ελαφρύ από άποψη ισχύος, μηχανισμό μηχανικής μάθησης. Ο μηχανισμός μηχανικής μάθησης παρατηρείται από πλευράς δέκτη αποτελεί πηγή εντροπίας, ισχυροποιώντας την λειτουργία των PUFs ως προς τον μηχανισμό ελέγχου ταυτότητας των πομπών. Ο δέκτης αποτελείται από ένα απλό νευρωνικό δίκτυο τριών επιπέδων, το οποίο έχει την ευθύνη για την αναγνώριση των πομπών. Η αναγνώριση επιτυγχάνεται από την διαδικασία της μηχανικής μάθησης, η οποία παράγει εκπαιδευτικά δεδομένα. Επομένως, όταν μία οντότητα κατορθώνει να επικοινωνήσει με τον δέκτη, ο δέκτης ανάλογα με τα εκπαιδευτικά δεδομένα του, αντιστοιχεί τις πληροφορίες και αναγνωρίζει τον πομπό [76,77,79]. (Sen, et al., 2008) (Banerjee, et al., 2014) (Suh, et al., 2007)

Πρόκληση (είσοδο) στην τεχνολογία αυτή, αποτελεί μία ψηφιακή ακολουθία. Σε αντίθεση με τις συμβατικές υλοποιήσεις PUFs, η απόκριση χαρακτηρίζεται από ένα αναλογικό ραδιοσήμα μοναδικό για κάθε πρόκληση. Ο δέκτης εκπαιδεύεται μέσω πολλών επαναλήψεων ψευδοτυχαίων ψηφιακών ροών bit, ώστε να αξιολογηθεί η μεταβλητότητα των δεδομένων κατά το στάδιο αξιολόγησης. Συνεπώς,

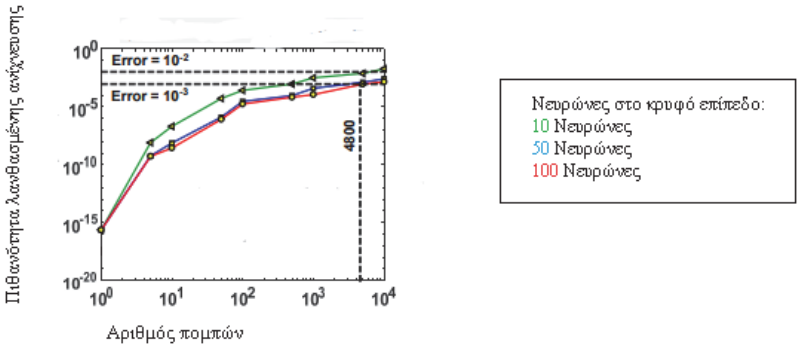
αντισταθμίζονται παραλλαγές καναλιού από την επαναληπτική ιδιότητα εκπαίδευσης του δέκτη.



Εικόνα 18: Εικονική αναπαράσταση του RF-PUF σε επίπεδο συστήματος[41].

Ωστόσο, και αυτό το ειδικά σχεδιασμένο PUF, αν και ισχυρότερο από άλλα συμβατικά PUFs, παρουσιάζει ευαισθησία σε επιθέσεις Μηχανικής Μάθησης, όπου ένας εισβολέας μπορεί να μοντελοποιήσει απαντήσεις (αποκρίσεις). Η ενσωμάτωση ιδιοτήτων διαγραφής και πιστοποίησης αποτελούν αντίμετρο στις προαναφερθέντες επιθέσεις (μοντελοποίησης). Η πρώτη ιδιότητα από αυτές, διευκολύνει την ανίχνευση παραβιάσεων, αλλά απαιτεί επιπλέον κύκλωμα ελέγχου. Η ιδιότητα της πιστοποίησης αφορά στον έλεγχο μίας απόκρισης για πιθανή παραβίαση, το οποίο απαιτεί πρόσθετα κυκλώματα. Η αποτελεσματική εφαρμογή του RF-PUF προϋποθέτει τις παραπάνω δύο ιδιότητες. Παρόλα αυτά, αυτή η ειδικά σχεδιασμένη PUF αποτελεί μία χαμηλού χρηματικού κόστους καλή λύση στα πλαίσια της ασφάλειας για τα συστήματα IoT· αυτό διότι επιτρέπει την αναγνώριση κόμβων σε πραγματικό χρόνο και έλεγχο ταυτότητας βασισμένο στις εγγενείς ιδιότητες των ραδιοσυχνοτήτων που δεν απαιτούν πρόσθετο υλικό και χαρακτηρίζονται από μικρές απαιτήσεις σε ισχύ [73,78,80]. (Chatterjee, et al., 2018) (Delvaux, et al., 2013) (Ruhrmair, et al., 2013).

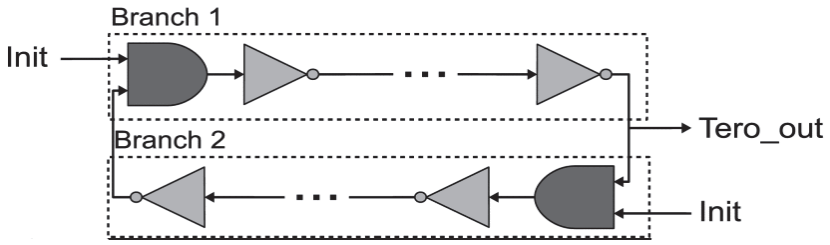
[41] https://arxiv.org/ftp/arxiv/papers/1805/1805.01048.pdf



Γράφημα 17: Πιθανότητα λανθασμένης ανίχνευσης πομπού, ως συνάρτηση του συνολικού αριθμού πομπών στο σύστημα[42].

4.7 TERO-PUF

Ειδικά σχεδιασμένο PUF συντελεί το TERO-PUF, τεχνολογία παρόμοια με το RO PUF με τη διαφορά ότι χρησιμοποιεί κελιά TERO που έχουν δύο πιθανές καταστάσεις. Μία εκ των δύο πιθανών καταστάσεων, είναι μια μεταβατική κατάσταση ταλάντωσης. Η παραπάνω κατάσταση χαρακτηρίζεται από τη συχνότητα ταλάντωσης της εξόδου κυττάρου και από τον αριθμό των ταλαντώσεων πριν από την επίτευξη σταθερή κατάσταση. Η δεύτερη πιθανή κατάσταση είναι η «σταθερή κατάσταση», που χαρακτηρίζεται από τη λογική τιμή της εξόδου του κελιού TERO. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)



Εικόνα 19: Γενική δομή του κελιού TERO[43]. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)

[42] https://arxiv.org/ftp/arxiv/papers/1805/1805.01048

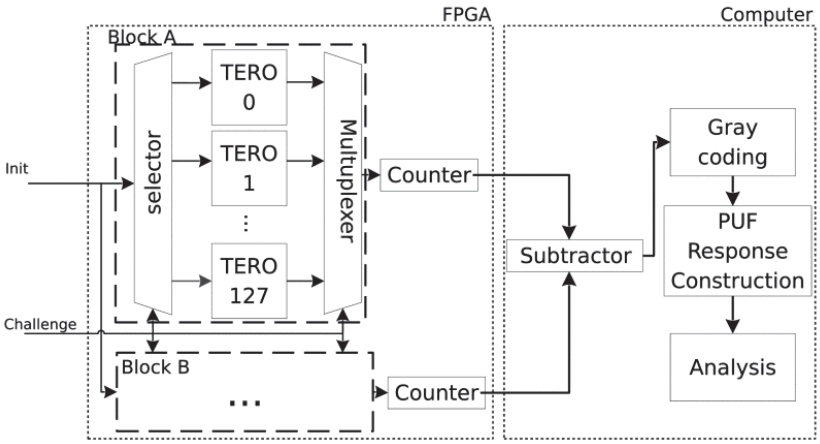
Όταν το κελί αρχικοποιείται[44], ξεκινούν να διαδίδονται δύο γεγονότα μέσα στο κελί TERO και αρχίζουν να ταλαντεύονται. Ανάλογα με την αναντιστοιχία στις καθυστερήσεις μεταξύ των δύο κλάδων του κελιού TERO που προκαλούνται από παραλλαγές στη διαδικασία CMOS, αυτά τα δύο συμβάντα μετακινούνται μέσα μέχρι να συγκρουστούν και να σταματήσουν την κατάσταση ταλάντωσης. Η συμπεριφορά αυτή, οδηγεί σε έναν πεπερασμένο αριθμό ταλαντώσεων της εξόδου κυττάρων TERO. Ο αριθμός των παροδικών ταλαντώσεων αυξάνεται με τον αριθμό των μετατροπέων σε κάθε κλάδο του κυττάρου TERO. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)

Η εφαρμογή του κελιού TERO σε FPGAs, προυποθέτει: ο αριθμός των μετατροπέων πρέπει να είναι ακριβώς ο ίδιος στα δύο κλαδιά του κελιού και, επίσης, όλες οι συνδέσεις μεταξύ των διαφόρων στοιχείων πρέπει να είναι ισοδύναμες. Δηλαδή, για παράδειγμα, η καθυστέρηση στη σύνδεση μεταξύ του σταδίου προετοιμασίας (And) και του πρώτου μετατροπέα πρέπει να είναι η ίδια και στους δύο κλάδους. Τέλος, οι συνδέσεις που συνδέουν τους δύο κλάδους πρέπει να είναι ίσες ώς προς την καθυστέρηση. Η εύρεση μιας υλοποίησης που να ταιριάζει με όλους τους περιορισμούς δεν είναι εύκολη στην πράξη. Ο περιορισμός που σχετίζεται με με την ισότητα του αριθμού των μετατροπέων στα δύο κλαδιά είναι δύσκολος με τα Altera FPGAs. Επιπρόσθετα, οι περιορισμοί ώς προς όλες τις συνδέσεις των στοιχείων και ώς προς τις συνδέσεις των δύο κλάδων είναι ιδιαίτερα απαιτητικοί με όλα τα SRP FPGAs.

Στην παρακάτω εικόνα δίνεται η δομή του TERO-PUF:

[43] https://ieeexplore.ieee.org/abstract/document/7922497

[44] άνοδο του σήματος "init"



Εικόνα 20: Αρχιτεκτονική υλικού / λογισμικού του TERO-PUF FPGA[45]. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)

Από την πλευρά του υλικού, εφαρμόζονται δύο μπλοκ από 128 κελιά TERO μαζί με δύο δυαδικούς μετρητές 16-bit. Για την επιλογή ενός κελιού TERO ανά μπλοκ, εφαρμόζονται επίσης δύο επιλογείς και δύο πολυπλέκτες. Αυτοί, τοποθετούνται μετά τα μπλοκ TERO κελιού ώστε να ακολουθήσει η σωστή έξοδος TERO στο ρολόι των μετρητών. Ως εκ τούτου, όταν αποστέλλεται μια πρόκληση στη συσκευή, μόνο δύο κύτταρα TERO ταλαντώνονται και ο αριθμός ταλαντώσεων τους επιστρέφεται από το FPGA.

Από την πλευρά λογισμικού, αφαιρείται ο αριθμός των ταλαντώσεων που λαμβάνονται από τη δοκιμαστική συσκευή και το αποτέλεσμα κωδικοποιείται χρησιμοποιώντας τον κώδικα Gray[46]. Από αυτήν τη διαφορά μεταξύ του αριθμού των ταλαντώσεων των δύο κυττάρων TERO, μπορούν να επιλεγούν bits για την παραγωγή της απόκρισης PUF.

Κάθε μπλοκ κελιών TERO περιέχει ακριβώς 128 κελιά (βλ. Εικόνα 20). Έτσι, ο αριθμός των πιθανών προκλήσεων (ζεύγη κυττάρων TERO) είναι 128 * 128 = 16.384 και ο αριθμός των πλήρως ανεξάρτητων συνόλων 128 προκλήσεων είναι 128. Είναι δυνατόν να δημιουργηθούν περισσότερες υπογραφές, αλλά θα έχουν κάποιο κοινό υποσύνολο προκλήσεων.

[45] https://ieeexplore.ieee.org/abstract/document/7922497

[46] Ο κώδικας "Gray" είναι δυαδικό σύστημα αρίθμησης με βασικό χαρακτηριστικό την μεταβολή ενός ψηφίου (bit) σε διαδοχικούς αριθμούς. Σε αντίθεση με την κανονική δυαδική αρίθμηση, κάθε ψηφίο δεν έχει σταθερή "αξία".

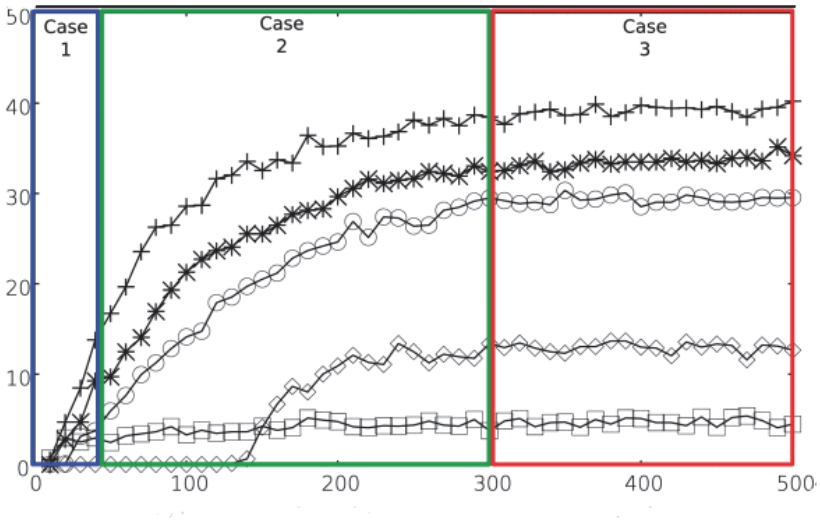
Χρησιμοποιώντας το TERO-PUF για την δημιουργία υπογραφών 128-bit, απαιτείται η χρήση πολλαπλών ζευγών CRP. Η απόκριση σε μία πρόκληση αντιστοιχεί σε ορισμένα επιλεγμένα κομμάτια της διαφοράς μεταξύ του αριθμού των ταλαντώσεων μεταξύ των δύο επιλεγμένων κυττάρων TERO. Ως εκ τούτου, δεν είναι δυνατή η εξαγωγή 128-bit χρησιμοποιώντας μόνο μία πρόκληση. Αρχικά, για τη δημιουργία πλήρων υπογραφών επιλέγονται ποιά είναι τα bit που χρησιμοποιούνται ως απόκριση μιας πρόκλησης. Με το PUF, δίνεται η δυνατότητα εξαγωγής από ένα έως τρία αξιόπιστα κομμάτια της διαφοράς μεταξύ του αριθμού των ταλαντώσεων των δύο κυττάρων που επιλέχθηκαν από την πρόκληση. Ακολούθως, είναι δυνατό να δημιουργηθούν υπογραφές με πολλούς διαφορετικούς τρόπους.

Το TERO-PUF χαρακτηρίζεται από τρεις βασικές μετρήσεις που ονομάζονται μοναδικότητα, αξιοπιστία και τυχαιότητα. Με αυτές, είναι δυνατό να εκτιμηθεί η ανθεκτικότητα του PUF ανάλογα με τις διακυμάνσεις της θερμοκρασίας ή της τάσης.

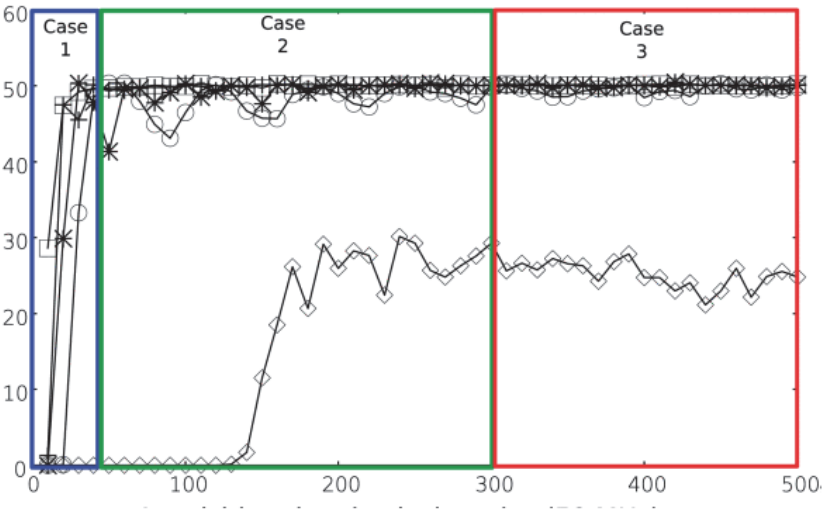
Πειραματικά, χρησιμοποιώντας Xilinx Spartan 6 FPGAs με πολύ μεγάλο acquisition window, παρατηρείται ότι ορισμένα κελιά TERO φάνηκαν να ταλαντεύονται επ 'αόριστον. Αυτό είχε σαν αποτέλεσμα, ο χρόνος απόκρισης του TERO-PUF ήταν πολύ μεγάλος. Ιδανικά, αυτά τα κελιά πρέπει να απορριφθούν από το σχήμα δημιουργίας απόκρισης. Η μοναδικότητα φτάνει στο 50%, παρόλο που τα κύτταρα TERO δεν έχουν φτάσει στη σταθερή τους κατάσταση. Επιπρόσθετα, όσο μικρότερο είναι το acquisition window, τόσο καλύτερη είναι η αξιοπιστία των αποκρίσεων PUF.

Ωστόσο, για το acquisition window, είναι απαραίτητο να γίνει διάκριση μεταξύ τριών διαφορετικών περιπτώσεων. Η πρώτη περίπτωση είναι ένα acquisition window που είναι τόσο σύντομο που κανένα κελί TERO δεν μπορεί να φτάσει στη σταθερή του κατάσταση πριν από το τέλος του. Σε αυτήν την περίπτωση, η αξιοπιστία των απαντήσεων PUF αναμένεται να είναι πολύ καλή, αντιθέτως με την τιμή της μοναδικότητα που δεν θα είναι αρκετή. Επίσης, ένα πολύ μικρό acquisition window υποδηλώνει ότι μπορούν να χρησιμοποιηθούν μόνο οι συχνότητες των κελιών του. Η δεύτερη περίπτωση είναι ένα acquisition window που είναι αρκετά μεγάλο για να αφήσει την πλειονότητα των κελιών TERO να φτάσουν στη σταθερή τους κατάσταση πριν τελειώσει. Η τρίτη και τελευταία περίπτωση αντιστοιχεί σε ένα πολύ μεγάλο acquisition window και όλα τα κελιά TERO φτάνουν στη σταθερή τους κατάσταση πριν τελειώσει.

Παρακάτω, παρατίθενται τα γραφήματα των αλλαγών στη σταθερότητα και τη μοναδικότητα με διακυμάνσεις στο χρόνο απόκτησης. Κάθε χρωματισμένο παράθυρο είναι τα προανεφερόμενα acquisition windows.



Γράφημα 18: Αξιοπιστία σε συνάρτηση με διακυμάνσεις στο χρόνο απόκτησης σε κύκλους ρολογιού στα 50 MHz[47]. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)



Γράφημα 19: Μοναδικότητα σε συνάρτηση με των χρόνο απόκτησης σε κύκλους ρολογιού στα 50 MHz[48]. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)

[47] https://ieeexplore.ieee.org/abstract/document/7922497
[48] https://ieeexplore.ieee.org/abstract/document/7922497

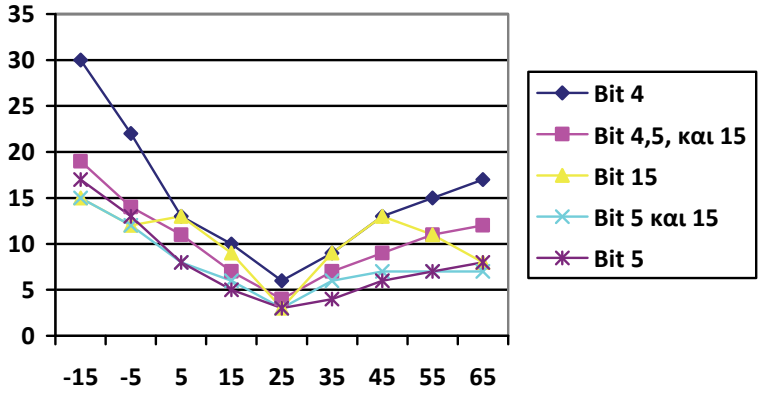
Πειραματικά, για την ανάδειξη των δυνατοτήτων του TERO-PUF χρησιμοποιήθηκαν από μελετητές 30 Xilinx Spartan 6 FPGAs (XC6SLX16CSG324-3). Όλες οι απαντήσεις PUF έχουν μήκος 128 bit. Το σύστημα απόκτησης χρησιμοποιεί δύο μετρητές 16-bit για να εξαγάγει τον αριθμό ταλαντώσεων των κελιών TERO. Το bit που αναφέρεται ως bit 0 αντιπροσωπεύει το λιγότερο σημαντικό bit και το bit που αναφέρεται ως Bit 15 αντιπροσωπεύει το σημαντικότερο bit της εξόδου.

Bit	Μοναδικότητα (%)	Αξιοπιστία (%)
0	47.65	28.41
1	42.37	23.02
8	0	0
15	48.46	2.63

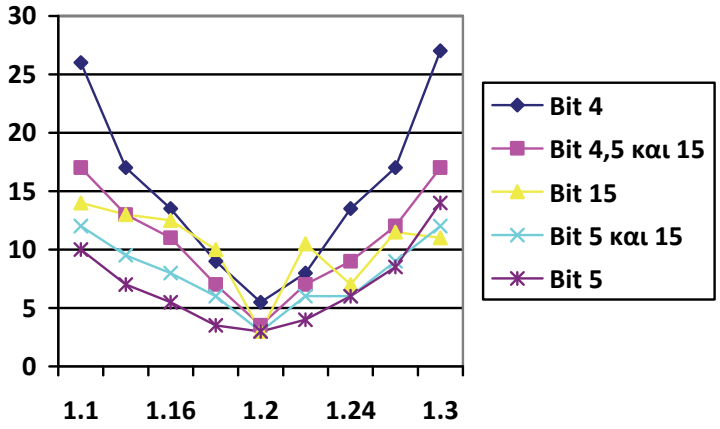
Πίνακας 4: Μοναδικότητα και Αξιοπιστία του αναγνωριστικού τσιπ 128 bit που δημιουργήθηκε χρησιμοποιώντας ένα κομμάτι της εξόδου σε Xilinx Spartan 6 FPGA χρησιμοποιώντας ένα acquisition window 30 κύκλων ρολογιού στα 50 MHz[49].

Τα παρακάτω γραφήματα παρουσιάζουν τα αποτελέσματα της αντοχής σε διακυμάνσεις θερμοκρασίας και τα αποτελέσματα της αντοχής σε διακυμάνσεις τάσης. Και στα δύο γραφήματα, αναγράφονται τα αποτελέσματα για τα bits 4, 5 και 15. Αυτά τα αποτελέσματα δημιουργήθηκαν χρησιμοποιώντας ένα acquisition window 30 κύκλων ρολογιού στα 50 MHz.

[49] https://ieeexplore.ieee.org/abstract/document/7922497



Γράφημα 20: Αξιοπιστία TERO-PUF σε διακυμάνσεις της θερμοκρασίας χρησιμοποιώντας ένα acquisition window 30 κύκλων ρολογιού στα 50 MHz στα Xilinx Spartan 6 FPGA[50].



Γράφημα 21: Αξιοπιστία TERO-PUF σε διακυμάνσεις τάσης χρησιμοποιώντας ένα acquisition window 30 κύκλων ρολογιού στα 50 MHz στα Xilinx Spartan 6 FPGAs[51].

Από τις γραφικές αναπαραστάσεις 20 και 21, η σταθερότητα της χειρότερης απόκρισης είναι μικρότερη από 10% μεταξύ 15 ° C και 35 ° C, η οποία αντιστοιχεί σε μεταβολή 40% περίπου Tn = 25 ∘C για μεταβολές στη θερμοκρασία. Το Γράφημα 20 παρουσιάζει ότι η σταθερότητα των αποκρίσεων είναι μικρότερη από 10% μόνο μεταξύ 1,18 και 1,22 V για μεταβολές στην τάση, η οποία αντιστοιχεί σε διακύμανση 1,5% περίπου Vn = 1,2 V. Έτσι, η ευαισθησία του TERO-PUF σε παραλλαγές στη

[50] https://ieeexplore.ieee.org/abstract/document/7922497
[51] https://ieeexplore.ieee.org/abstract/document/7922497

θερμοκρασία είναι χαμηλή, αλλά είναι πιο ευαίσθητη σε διακυμάνσεις τάσης. Οι χειρότερες αποκρίσεις αντιστοιχούν σε αυτές που δημιουργούνται χρησιμοποιώντας μόνο το bit 4 της εξόδου για αντοχή σε μεταβολές στη θερμοκρασία και σε αποκρίσεις που δημιουργούνται χρησιμοποιώντας το bit 15 της εξόδου για την ανθεκτικότητα στις διακυμάνσεις της τάσης [99][100]. (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)(Michailidis, Kogias, & Voyiatzis, 2020)

Στον παρακάτω πίνακα παρουσιάζεται η τυχαιότητα των αποκρίσεων TERO PUF χρησιμοποιώντας 1 έως 3 Bits ανά πρόκληση με acquisition window 60 κύκλων ρολογιού στα 50 MHz σε Xilinx Spartan 6 FPGA.

Bit	Αξιοπιστία (%)	Μοναδικότητα (%)	Tests					
			T1	T2	T3	T4	T5	T6
5	10.17	49.88	X	Na	X	X	X	X
6	5.09	49.88	X	Na	X	X	X	X
15	2.38	49.37	X	Na	X	X	X	X
5 & 15	6.08	49.51	X	X	X	X	X	X
6 & 15	3.68	49.65	X	X	X	X	X	X
5,6 & 15	5.89	49.49	X	X	X	X	X	X

Πίνακας 5: Τυχαιότητας αποκρίσεων TERO PUF χρησιμοποιώντας 1 έως 3 Bits ανά πρόκληση με ένα acquisition window 60 κύκλων ρολογιού στα 50 MHz σε Xilinx Spartan 6 FPGA[52].

Είναι δυνατή η δημιουργία αποκρίσεων χρησιμοποιώντας ένα, δύο ή τρία bits της διαφοράς μεταξύ του αριθμού των ταλαντώσεων των κυττάρων TERO χρησιμοποιώντας αυτό το acquisition window 60 κύκλων ρολογιού στα 50 MHz. Συγκεκριμένα, η διαμόρφωση που χρησιμοποιεί τα bits 6 και 15 δείχνει πολύ καλή αξιοπιστία με τιμή 3,68% καθώς, και μοναδικότητα με τιμή 49,65%.

Η μοναδικότητα που παρουσιάζει το TERO-PUF είναι καλύτερη από αυτή του RO-PUF. Κατα αυτό το γεγονός, το TERO-PUF χαρακτηρίζεται από περισσότερη εντροπία από παραλλαγές στη διαδικασία κατασκευής συγκριτικά με το

[52] https://ieeexplore.ieee.org/abstract/document/7922497

RO-PUF. Ως προς την αξιοπιστία και οι δύο τεχνολογίες PUFs χαρακτηρίζονται από παραπλήσιες τιμές.

Μέτρο	**RO-PUF**	**TERO-PUF**
Τεχνολογία	Xilinx Spartan 6 (45nm)	Xilinx Spartan 6 (45nm)
Μοναδικότητα	55.5 %	48.5 %
Αξιοπιστία	2.5 %	2.6 %
Αρχιτεκτονική βασικών κελιών	1 AND και 3 inverters	2 AND και 14 inverters

Πίνακας 6: Σύγκριση RO-PUF και TERO-PUF με τεχνολογία Xilinx Spartan 6 (45nm)[53].

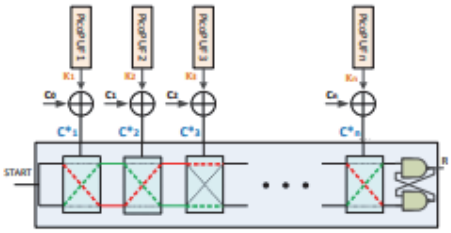
Για το IoT, το TERO-PUF έχει προβάδισμα έναντι συμβατικών υλοποιήσεων PUF, καθώς, είναι πιο ανθεκτικό στις ηλεκτρομαγνητικές επιθέσεις, δεν είναι ευαίσθητο στο φαινόμενο κλειδώματος και καταναλώνει λιγότερη ισχύ από το RO-PUF. Τα φαινόμενα κλειδώματος αντιστοιχούν στον χειρισμό της συχνότητας των κυμαινόμενων κυττάρων προκειμένου να τα αναγκάσουν να λειτουργήσουν σε μια συγκεκριμένη συχνότητα. Η αρχή του RO-PUF βασίζεται στην αναντιστοιχία συχνότητας θεωρητικά πανομοιότυπων κυττάρων. Στην περίπτωση του TERO-PUF, δεν αναλύεται η συχνότητα όπως στο RO-PUF, αλλά ο αριθμός των παροδικών ταλαντώσεων. Επιπρόσθετα, ο αριθμός των ταλαντώσεων είναι πεπερασμένος και ο χρόνος ταλαντώσεων είναι συνήθως πολύ μικρός. Έτσι, τα φαινόμενα κλειδώματος δεν θα έχουν αντίκτυπο στο TERO-PUF. Το TERO-PUF καθιστά δυνατή την εξαγωγή αρκετών bit ανά πρόκληση, γεγονός που οδηγεί σε αποτελεσματικότητα περιοχής. Το TERO-PUF είναι συνεπώς ελαφρύτερο από το RO-PUF όσον αφορά την κατανάλωση εμβαδού και ισχύος. Για το IoT το μέγεθος αλλά και η κατανάλωση ισχύος συνιστούν βασικούς περιορισμούς κατα την φάση σχεδιασμού των συσκευών του. Τέλος, τα PUF στο IoT αναλαμβάνουν την διαδικασία ελέγχου ταυτότητας συσκευών. Ως εκ τούτου, δεν υπάρχει μεγάλη ανάγκη για 100% αξιοπιστία. Χρησιμοποιώντας ελαφριά πρωτόκολλα μια συσκευή μπορεί να πιστοποιηθεί χωρίς τέλεια τιμή αξιοπιστίας. Εν κατακλείδι, εάν απαιτείται διόρθωση σφάλματος για τον έλεγχο ταυτότητας συσκευών, πρέπει να εφαρμοστεί στον διακομιστή ελέγχου

[53] https://ieeexplore.ieee.org/abstract/document/7922497

ταυτότητας και όχι σε chip [100][99]. (Michailidis, Kogias, & Voyiatzis, 2020) (Marchand, Bossuet, Mureddu, Bochard, Cherkaoui, & Fischer, Jan. 2018)

4.8 MPUF

Μία καλή προσέγγιση PUF για την αντιμετώπιση επιθέσεων μηχανικής μάθησης είναι η ειδικά σχεδιασμένη PUF, M-PUF. Η υλοποίηση αυτή, αποτελεί μία εξίσου ελαφριά λύση άμυνας, η οποία διακρίνεται από σημαντικά βελτιωμένη αντίσταση σε ML επιθέσεις. Πιο συγκεκριμένα, η MPUF χρησιμοποιεί αδύναμα PUF για να συγκαλύψει τις προκλήσεις για ένα ισχυρό PUF για την ενίσχυση της ασφάλειας έναντι επιθέσεων μοντελοποίησης. Ο προτεινόμενος σχεδιασμός MPUF έχει υψηλότερη πολυπλοκότητα συγκριτικά με συμβατικές υλοποιήσεις PUFs και, ως εκ τούτου, είναι πιο δύσκολο να δεχτεί επίθεση [103]. (Ma, Gu, Hanley, Wang, Liu, & &, 22 February 2018).

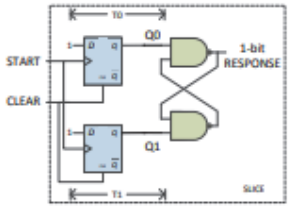


Εικόνα 21: Ο σχεδιασμός MPUF βασίσμένος σε PicoPUF και ένα PUF Arbiter[54].

Πειραματικά, μελετητές έδειξαν με δύο διαφορετικούς τύπους επιθέσεων μοντελοποίησης με βάση τη μηχανική μάθηση, δηλαδή λογιστική παλινδρόμηση (LR) και πίνακας συνδιακύμανσης στρατηγικής εξέλιξης προσαρμογής (CMA-ES), ότι το MPUF επιτυγχάνει ποσοστό πρόβλεψης 50% χρησιμοποιώντας LR σε σύγκριση με το 100% για το συμβατικό Arbiter PUF. Για μια πρόκληση 32-bit η επίθεση CMAES επιτυγχάνει επίσης ένα ποσοστό πρόβλεψης 100% για το συμβατικό Arbiter PUF, ενώ για το MPUF, ακόμη και με ένα μεγάλο σύνολο δειγμάτων 10.000 CRP, το ποσοστό πρόβλεψης είναι μικρότερο από 80%.

[54] https://ieeexplore.ieee.org/document/8297289

Ο σχεδιασμός MPUF βασίζεται σε PicoPUF και ένα PUF Arbiter. Το PicoPUF PUF παρουσιάζει υψηλή αξιοπιστία και μοναδικότητα. Ο σχεδιασμός ενός κελιού παραγωγής απόκρισης 1-bit έχει σχεδιαστεί για να ταιριάζει σε ένα κομμάτι FPGA, όπως φαίνεται σχηματικά στην παρακάτω Εικόνα.

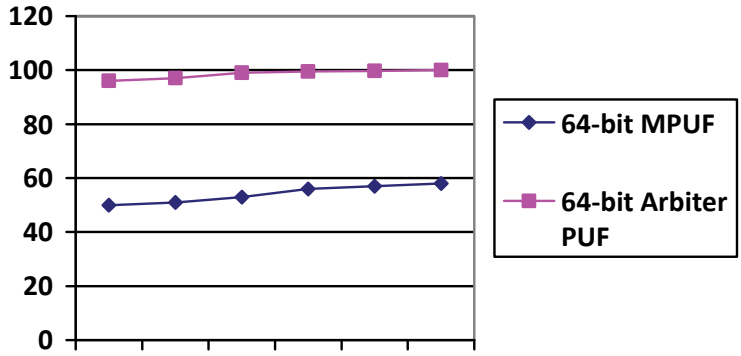


Εικόνα 22: Υλοποίηση PicoPUF[55].

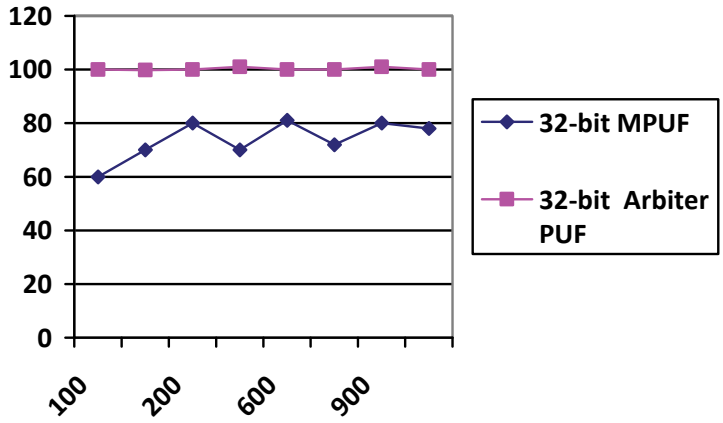
Το PicoPUF είναι ελαφρύ και μπορεί να τοποθετηθεί με ευελιξία οπουδήποτε σε ένα FPGA. Η δημιουργία μίας απάντηση bit, οφείλεται σε δύο αντιστοιχισμένες διαδρομές καθυστέρησης χρόνου, T0 και T1, που ενεργοποιούνται από δύο flip flops τύπου D ταυτόχρονα από το ανερχόμενο άκρο ενός σήματος START και συνδέονται με τους ακροδέκτες ρολογιού μετά την πρώτη επαναφορά από CLEAR. Λόγω της υποκείμενης παραλλαγής της διαδικασίας παραγωγής, οι χρόνοι διάδοσης των σημάτων στο πέρασμα των flip flops είναι διαφορετικοί. Έτσι, δημιουργεί μια κατάσταση αγώνα μεταξύ των δύο διαδρομών καθυστέρησης. Οι πύλες NAND μεταξύ ζευγών χρησιμοποιούνται ως κριτής ώστε να αποφασίσει ποίο σήμα έφτασε πρώτα και εμφανίζει την απόκριση ως δυαδική τιμή 0 ή 1 [103]. (Ma, Gu, Hanley, Wang, Liu, & &, 22 February 2018)

Στα παρακάτω Γραφήματα παρουσιάζονται τα ποσοστά πρόβλεψης για συμβατικά PUF Arbiter και ειδικά σχεδιασμένα MPUF από την επίθεση LR και από την CMA-ES.

[55] https://ieeexplore.ieee.org/document/8297289



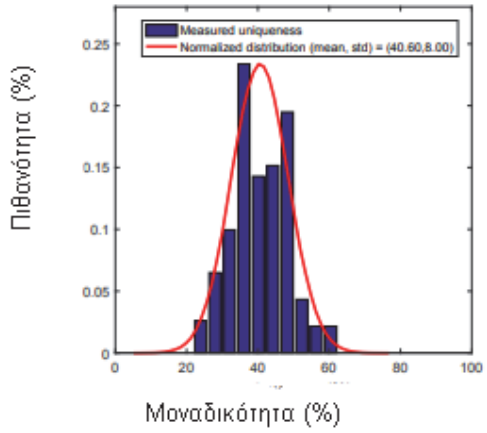
Γράφημα 22: Τα ποσοστά πρόβλεψης για συμβατικά PUF Arbiter και σχέδια MPUF από την επίθεση LR[56].



Γράφημα 23: Τα ποσοστά πρόβλεψης για συμβατικά PUF Arbiter και σχέδια MPUF από την επίθεση CMA-ES[57].

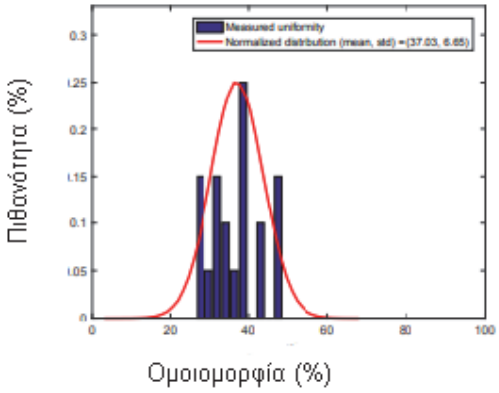
Το Γράφημα 24 περιλαμβάνει το αποτέλεσμα της μοναδικότητας για το MPUF έχει μέσο όρο 40,6% και τυπική απόκλιση 8%. Αυτό ισοδυναμεί με τη μοναδικότητα του flip flop με βάση το Arbiter PUF. Επιπρόσθετα, σε σύγκριση με τη μοναδικότητα, τα αποτελέσματα από 5,44% έως 10,82% που επιτεύχθηκαν από συμβατικές υλοποιήσεις PUF, ο σχεδιασμός MPUF επιδεικνύει σημαντικά υψηλότερη μοναδικότητα.

[56] https://ieeexplore.ieee.org/document/8297289
[57] https://ieeexplore.ieee.org/document/8297289



Γράφημα 24: Αποτέλεσμα της μοναδικότητας για το MPUF[58].

Η ομοιομορφία αντιπροσωπεύει το ποσοστό μηδενικών σε μια απόκριση PUF. Στην ιδανική περίπτωση θα πρέπει να είναι 50%, Όσο μεγαλύτερη ομοιομορφία, τόσο δυσκολότερο για έναν εισβολέα να μαντέψει την απάντηση μιας συσκευής. Το αποτέλεσμα ομοιομορφίας για τον σχεδιασμό MPUF φαίνεται στο Γράφημα 24 και έχει μέσο όρο στο 37,03% και τυπική απόκλιση στο 6,65%.



Γράφημα 25: Αποτέλεσμα της ομοιομορφίας για το MPUF[59].

Κλείνοντας, η αντίσταση που παρουσιάζει η υλοποίηση MPUF σε επιθέσεις μηχανικής μάθησης απεικονίζει τη σκοπιμότητα του σχεδιασμού για εφαρμογή της στο FPGA και στο IoT. Ο σχεδιασμός επιτυγχάνει ποσοστό πρόβλεψης 50%

[58] https://ieeexplore.ieee.org/document/8297289
[59] https://ieeexplore.ieee.org/document/8297289

χρησιμοποιώντας τη LR επίθεση σε σύγκριση με το 100% για την συμβατική υλοποίηση Arbiter PUF. Με την CMA-ES επίθεση, αν και η υλοποίηση MPUF μπορεί να προβλεφθεί επιτυχώς για ένα μικρό μέγεθος πρόκλησης, είναι πιο ανθεκτικό από το Arbiter PUF. Όμως, όταν το μέγεθος πρόκλησης αυξάνεται σε 32 bits, η επίθεση CMAES μπορεί να πετύχει μόνο ένα ποσοστό πρόβλεψης περίπου 80% για την υλοποίηση MPUF, ακόμη και με ένα μεγάλο σύνολο δειγμάτων 10.000 CRP. Σε αντίθεση με την συμβατική υλοποίηση Arbiter PUF που επιτυγχάνεται ποσοστό πρόβλεψης 100% [103]. (Ma, Gu, Hanley, Wang, Liu, & &, 22 February 2018)

ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΕΣ ΠΡΟΕΚΤΑΣΕΙΣ

Η ανάπτυξη και χρήση της τεχνολογίας του IoT προϋποθέτει την ασφάλεια όλων το δικτυωμένων συσκευών του. Οι συσκευές του παρουσιάζουν ιδιαίτερα χαρακτηριστικά σε σχέση με τα παραδοσιακά ψηφιακά συστήματα. Τα ιδιαίτερα χαρακτηριστικά αυτά αφορούν στην χαμηλή κατανάλωση ενέργειας, την περιορισμένη ισχύ και τη μνήμη, το μέγεθος των συσκευών (μικροσυσκευές), την περιορισμένη υπολογιστική ισχύ και τέλος, το χαμηλό κόστος τους. Ως εκ τούτου, συμβατοί μηχανισμοί ασφαλείας δεν ενδείκνυται για την «θωράκιση» του IoT από επιθέσεις. Χαρακτηριστικό παράδειγμα, η χρήση κλασικών ασφαλών κρυπτογραφικών αλγορίθμων καθίστανται απαγορευτικοί για τα συστήματα IoT, λόγω του μεγάλου κόστους, της μεγάλης απαίτησης σε υπολογιστική ισχύ και των σχετικά μεγάλων απαιτήσεων σε μνήμη. Οι PUFs αποτελούν μία εναλλακτική λύση, η οποία χαρακτηρίζεται από μικρές απαιτήσεις σε ισχύ και μνήμη. Η τεχνολογία αυτή επιτρέπει την ασφαλή αναγνώριση αντικειμένων, παρέχει μηχανισμό ελέγχου ταυτότητας με χαμηλό κόστος, καθώς και σχήματα κρυπτογράφησης αξιοποιώντας τα χαρακτηριστικά του υλικού των τσιπ στα ολοκληρωμένα κυκλώματα. Ωστόσο, τα ιδιαίτερα χαρακτηριστικά των συσκευών του IoT σε συνδυασμό με ευπάθειες σε επιθέσεις που έχουν παρουσιάσει οι PUF, κρίνουν σκόπιμη την χρήση ειδικά σχεδιασμένων PUFs για τα συστήματα IoT. Ερευνητικές δραστηριότητες πάνω στις PUFs στο IoT τείνουν να αντιμετωπίσουν ευαισθησίες τους, με απώτερο σκοπό την εφαρμογή τους στο IoT στα πλαίσια της ασφάλειας. Οι PUFs αυτές χαρακτηρίζονται από μεγαλύτερη ανθεκτικότητα σε επιθέσεις και είναι πιο συμβατές με τις κατασκευαστικές ιδιαιτερότητες των συσκευών του IoT. Τέτοιες τεχνολογίες αποτελούν οι LHPUF, PUF-IPA, C-PUF, PPUF, RF-PUF, TERO PUF, MPUF και τα PUF που βασίζονται στην μνήμη. Πειραματικά, αποδεικνύεται ότι αυτές οι ειδικά σχεδιασμένες τεχνολογίες PUFs είναι αποδοτικές και αξιόπιστες λύσεις ασφαλείας χαμηλού κόστους διατηρώντας το απόρρητο των συσκευών.

Ειδικά σχεδιασμένο PUF	Αντίμετρο σε Επίθεση
LHPUF	Πλευρικού καναλιού
PUF-IPA	Μηχανική Μάθηση
Mem-APUF	Hardware Trojan
C-PUF	Man in the Middle
PPUF	Πλευρικού καναλιού
RF-PUF	Πλευρικού καναλιού
TERO PUF	Hardware Trojan
MPUF	Μηχανική Μάθηση

Πίνακας 7: Ειδικά σχεδιασμένες PUFs ώς αντίμετρα σε επιθέσεις.

Παρά το γεγονός ότι νέες τεχνολογίες PUFs κερδίζουν κάποια δημοσιότητα και παρουσιάζουν όλο και μεγαλύτερη αξιοπιστία ώς προς την ασφάλεια στο IoT, δεν μπορούν να αντιδράσουν αποτελεσματικά σε νέες αναπτυσσόμενες επιθέσεις. Έως και σήμερα, δεν έχει αναπτυχθεί πρωτόκολλο που αντιμετωπίζει πλήρως όλες τις προκλήσεις που έχει θέσει το IoT. Είναι σημαντική η επανεξέταση των αρχικών στόχων της χρήσης PUFs στο IoT, έτσι ώστε αντί να αντικαθιστούν την κρυπτογραφία, να λειτουργούν συνδυαστικά. Ως εκ τούτο, κρίνεται σημαντική η ανάπτυξη ενός «ελαφρού» κρυπτογραφικού μοντέλου που θα λειτουργεί συνεργατικά με PUFs, τα οποία θα δημιουργούν «ισχυρά» κρυπτογραφικά κλειδιά, καλύτερους τυχαίους αριθμούς και θα συμβάλλουν αποτελεσματικά στην διαδικασία ελέγχου ταυτότητας. Επιπλέον, για το μετριασμό τρωτών σημείων που παρατηρήθηκαν σε υπάρχουσα φυσικά μέσα, αντίμετρα αποτελούν ο συνδυασμός λογισμικού και υλικού. Στα πλαίσια της ML, φαίνεται από μελέτες ότι ξεπεράστηκαν οι κίνδυνοι από τις απειλές Δούρειων Ίππων και αναμένεται ότι θα χρησιμοποιηθεί, για την ενίσχυση της διαδικασίας ελέγχου ταυτότητας [100]. (Michailidis, Kogias, & Voyiatzis, 2020)

ΒΙΒΛΙΟΓΡΑΦΙΑ

s.l. : http://www.reloade.com/blog/2013/12/6characteristics-within-internet-things-iot.php.

s.l. : https://www.ida.gov.sg/~/media/Files/Infocomm%20Lan.

A survey on Internet of Things: Architecture, Enabling Technologies, Security andPrivacy, and Applications. **Lin, J., και συν. 2017.** 38–60, s.l. : IEEE Internet of Things , 2017, Τόμ. Journal 4. 5.

Akinaga, H. και Shima, H. 2010. *Resistive Random Access Memory (ReRAM) based on Metal Oxides.* s.l. : IEEE, 2010. σσ. 2237–2251.

Angelakis, V., και συν. 2017. *Designing,Developing, and Facilitating Smart Cities: Urban Design to IoT Solutions.* Switzerland : s.n., 2017.

Ashton, K. 2009. *That 'Internet of Things' Thing. RFID.* 2009.

Atlam, H.F., Walters, R.J και Wills, G.B. 2018. *Internet of things: state-of-the-art, challenges, applications, and open issues.* 2018.

Atlam, Hany F. και Wills, Gary. 2019. *IoT Security, Privacy, Safety and Ethics.* 2019.

Atzori, L., Iera, A. και Morabito, G. 2010. *The Internet of Things: A Survey.* 2010.

B. Gassend, D. Clarke, Dijk, M. Van και Devadas, S. 2002. *Controlled physical.* s.l. : IEEE, 2002.

Babaei, A. και Schiele, G. 2019. *Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges.* s.l. : Sensors 19, 2019.

Babaei, Armin και Schiele, Gregor. 2019 . *Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges.* Duisburg : MDPI, 2019 .

Banerjee, D., και συν. 2014. *SelfLearning MIMO-RF Receiver Systems: Process Resilient Real-time Adaptation to Channel Conditions for Low Power Operation.* 2014.

Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff. 1999. *A Brief History of Internet.* s.l. : https://el.wikipedia.org/wiki/ArXiv ; http://arxiv.org/abs/cs/9901011, 1999.

Beckmann, N. και Potkonjak, M. 2009. *Hardware-based public-key cryptography with public physically unclonable functions, in: International Workshop on Information Hiding.* s.l. : Springer, 2009.

BI Intelligence. 2016. s.l. : Βασίλης Ζεϊμπέκης, Ph.D, 2016.

Borgohain, T., U., Kumar και S. Sanya. 2015. *Survey of security and privacy issues of internet of things.* s.l. : arXiv preprint arXiv:1501.02211, 2015.

Botta, A. 2016. *Integration of cloud computing and internet of things: a survey.* 2016.

Braeken. 2018. *PUF Based Authentication Protocol for IoT.* Brussel : MDPI, 2018.

Burg, A., Chattopadhyay, A. και Lam, K.-Y. 2018. *Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things.* s.l. : IEEE, 2018.

Cao, Y., και συν. 2015. *A low-power hybrid ro puf with improved thermal stability for lightweight applications.* s.l. : IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst, 2015.

Capra, Maurizio, και συν. 27 March 2019. *Edge Computing: A Survey On the Hardware Requirements in the Internet of Things World.* Torino : s.n., 27 March 2019.

Chatterjee, B., Das, D. και Sen, S. 2018. *RF-PUF: IoT Security Enhancement through Authentication of Wireless Nodes using In-situ Machine Learning.* s.l. : IEEE, 2018.

Chatterjee, Baibhab και Maity, Shovan. 2018. *RF-PUF: Enhancing IoT Security through Authentication of Wireless Nodes using In-situ Machine Learning .* s.l. : IEEE, 2018.

Chen, D., και συν. 2011. *A Novel Secure Architecture for the Internet of Things, in: Genetic and Evolutionary Computing.* s.l. : IEEE, 2011.

Chen, M. και Chen, S. 2016. *RFID Technologies for Internet of Things.* Switzerland : AG, 2016.

Delvaux, J. και Verbauwhed, I. 2013. *Side Channel Modeling Attacks on 65nm Arbiter PUFs Exploiting CMOS Device Noise.* s.l. : IEEE, 2013.

Department, Computer Science, Carnegie και Mellon. 1998. *The "Only" Coke Machine on the Internet.* s.l. : https://www.cs.cmu.edu/~coke/history_long.txt, 1998.

Du, X., Le-Khac, N.A. και Scanlon, M. 2017. *Evaluation of digital forensic process models with respect to digital forensics as a service.* Dublin : ECCWS, 2017.

Featherly, Kevin. ARPANET. [συγγρ. βιβλίου] Featherly Kevin. *Encyclopaedia Britannica.*

Finkenzeller, K. και Müller, D. 2010. *RFID Handbook. Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication.* s.l. : John Wiley ; Sons, 2010.

Floerkemeier, Christian, και συν. 2008. *The Internet of Things.* Zurich : SpringerLink, 2008.

Gassend, Blaise, και συν. November 2002. *Silicon Physical Random Functions. Proceedings of the Computer and Communications Security Conference* . November 2002.

Genc, Hasan, και συν. 2015. *Flying IoT: Toward Low-Power Vision in the Sky.* s.l. : IEEE, 2015.

Gubbi, Jayavardhana, και συν. 2013-09-01. A vision, architectural elements, and future directions. [συγγρ. βιβλίου] Rajkumar Buyya, Slaven Marusic, M. Palaniswami Jayavardhana Gubbi. *Internet of Things.* s.l. : https://www.sciencedirect.com/science/article/pii/S0167739X13000241, 2013-09-01, σσ. 1645–1660.

—. September 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. [συγγρ. βιβλίου] Anup Kumar, Chi-Ming Chen, Suraj Pandey, Surya Nepal Bin Xie. *Future Generation Computer Systems.* September 2013, σσ. 1645-1870 .

Ha, J., και συν. 2007. *Low-cost and strong-security RFID authentication protocol. Emerging Directions in Embedded and Ubiquitous Computing.* s.l. : https://pdfs.semanticscholar.org/e2b5/0a448e78d91c7e7cc904fddbac07aac449fb.pdf, 2007.

Halak, Basel, Zwolonski, Mark και Mispan, M. Syafiq. 16-19 Oct. 2016. *Overview of PUF-based hardware security solutions for the internet of things.* s.l. :

2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS), 16-19 Oct. 2016.

Helfmeier, C., και συν. 2014. *Physical Vulnerabilities of Physically Unclonable Functions, in: Proceedings of the conference on Design.* 2014.

2018-02-01. *Internet of Things (IOT)* . s.l. : https://www.sas.com/el_gr/insights/big-data/internet-of-things.html, 2018-02-01.

i-TECH4u.gr. 2018-02-02. *Internet of Things σε απλά ελληνικά.* s.l. : https://web.archive.org/web/20180202162428/http://www.itech4u.gr/tech/hands-on/item/7262-internet-of-things-se-apla-ellinika/7262-internet-of-things-se-apla-ellinika, 2018-02-02.

Jan, Mian Ahmad, και συν. 2017. *A payload-based mutual authentication scheme for Internet of Things.* s.l. : https://www.researchgate.net/, 2017.

Karlof, C. και Wagner, D. 14 December 2018. *Secure routing in wireless sensor networks: Attacks and countermeasures.* s.l. : http://www.chriskarlof.com/papers/senroute-adnj.pdf, 14 December 2018.

Karri, R., και συν. 2010. *Trustworthy Hardware: Identifying and Classifying Hardware Trojans* . s.l. : Computer 43, 2010.

Khattab, A., και συν. 2017. *RFID Security. A Lightweight Paradigm.* USA : s.n., 2017.

LeadingEdge. *Cloud Deployment Models.* s.l. : https://www.leadingedgetech.co.uk/it-services/it-consultancy-services/cloud-computing/what-are-the-types-of-cloud-computing/.

M. Rostami, F. Koushanfar, R. Karri. 2014. *A Primer on Hardware Security: Models, Methods, and Metrics.* s.l. : IEEE, 2014.

Maes, R. 2012. *Physically Unclonable Functions: Constructions, Properties.* s.l. : KU Leuven, 2012.

Magrassi, Paolo. 2001. *A World Of Smart Objects: The Role Of Auto.* 2001.

Mattern, Friedemann και Floerkemeier, Christian. 2010. *From the Internet of.* 2010.

Mavromoustakis, C, Mastorakis, G και Dobre, C. 2017. *Advances in Mobile Cloud Computing and Big Data in the 5G.* UK : s.n., 2017.

Mavromoustakis, και συν. 2017. *Advances in Mobile Cloud Computing and Big Data in the 5G.* UK : s.n., 2017.

Miorandi, D., και συν. 2012. *Internet of Things:Vision, applications and research challenges.* s.l. : Ad Hoc Networks, 2012.

Oreku, G. και Pazynyuk, T. 2016. *Security in Wireless Sensor Networks.* Switzerland : s.n., 2016.

Panicker, Pravinraj. 2020. *Bluetooth vs Wifi for the Internet of Things (IoT).* s.l. : https://www.quicsolv.com/blog/internet-of-things/bluetooth-vs-wifi-comparison-iot-solutions/, 2020.

Pate, Keyur και Patel, S. 2016. *Internet of Things-IOT : Definition , Characteristics , Architecture , Enabling Technologies , Application & Future Challenges.* s.l. : https://www.semanticscholar.org, 2016.

Patel, Keyur K, Patel, Sunil M and Salazar, Carlos. May 2016. Internet of Things-IOT: Definition, Characteristics, Architecture,Enabling Technologies, Application & Future Challenges. May 2016, Vol. 6, 5.

Patil, Akash Suresh, και συν. 2020. *Blockchain-PUF-Based Secure Authentication Protocol for Internet of Things.* s.l. : SprinerLink, 2020.

—. 2020. *Blockchain-PUF-Based Secure Authentication Protocol for Internet of Things.* s.l. : SpringerLink, 2020.

Pews Research Center. 11 Μαρτίου 2014. *Word Wide Web Timeline.* 11 Μαρτίου 2014.

Postel, J. May 28, 2009. *NCP/TCp to the Internet.* s.l. : 2. RFC 801, May 28, 2009.

Qureshi, Mahmood Azhar και Munir, Arslan. 10-13 Jan. 2020. *PUF-IPA: A PUF-based Identity Preserving Protocol for Internet of Things Authentication.* s.l. : 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 10-13 Jan. 2020.

RIOT: An Open Source Operating System for Low-end Embedded Devices in the IoT. **Baccelli, E., και συν. 2018.** E Internet of Things Journal 5 , s.l. : IEEE, 2018, Τόμ. 5. 4428–4440.

Roberti, Mark. October 2013. *RFID, Sensors and the Internet of Things.* October 2013.

Rockerhousen, Nathan. 2016. *The internet of things and Bluetooth.* s.l. : http://gridconnect.com/blog/general/the-internet-of-things-and-bluetooth/, 2016.

Rohatgi, P. 2009. *Electromagnetic Attacks and Countermeasures, in: Cryptographic Engineering.* s.l. : Springer, 2009.

Rose, Karen, Eldridg, Scott και Chapin, Lyman. 2015. *Internet of Things – An.* 2015.

Ruhrmair, U. και Dijk, M. van. 2013. *"PUFs in Security Protocols: Attack Models and Security Evaluations.* s.l. : IEEE, 2013.

Sankaran, Sriram, Shivshankar, S. και Nimmy, K. 17-19 Dec. 2018. *LHPUF: Lightweight Hybrid PUF for Enhanced Security in Internet of Things.* s.l. : IEEE, 17-19 Dec. 2018.

Sarma, et, al.

Schlosser, A., και συν. 2013. *Simple Photonic Emission Analysis of AES, Journal of Cryptographic Engineering 3.* 2013.

Sen, S., και συν. 2008. *Pro-VIZOR:Process Tunable Virtually Zero Margin Low Power Adaptive RF for Wireless Systems.* 2008.

Shamsoshoara, Alireza, και συν. 2020. *A survey on physical unclonable function (PUF)-based security solutions for Internet of Things.* s.l. : ScienceDirect, 2020.

Soro, Brereton και Roe. 2018 . *Social Internet of Things.* Switzerland : s.n., 2018 .

Stallings, W. 2015. *The internet of things: network and security architecture.* 2015.

Stergiou, Christos, Kim, Byung-Gyu και Psannis, Kostas E. 2016. *Secure Integration of Internet-of-Things and Cloud Computing* . s.l. : https://www.researchgate.net/deref/http%3A%2F%2Fwww.elsevier.com%2Flocate%2Ffgcs, 2016.

Suh, G. και Devadas, S. 2007. *Physical Unclonable Functions for Device Authentication and Secret Key Generation.* 2007.

Susan R. Harris, Ph.D., and Elise Gerich, ConneXions. 4, April 1996. *Retiring the NSFNET Backbone Servece.* s.l. : http://merit.edu/research/nsfnet_article.php, 4, April 1996.

Tehranipoor, M. και Koushanfar, F. 2010. *A Survey of Hardware Trojan Taxonomy and Detection.* s.l. : IEEE design & test of computers 27, 2010.

Tehranipoor, M. και Wang, C. 2011. *Introduction to hardware security and trust.* 2011.

Tripathy, BK και J Anuradha. 2018. *Internet of Things (IoT): Technologies, Applications,Challenges and Solutions.* USA : s.n., 2018.

Ullah, Saleem, και συν. 2017. *Security Issues in the Internet of Things (IoT): A Comprehensive Study.* s.l. : www.ijacsa.thesai.org, 2017.

Vermesan, Dr. Ovidiu και Friess, Dr. Peter. 2013. *"Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems.* Norway : s.n., 2013.

Wen, Sheng, Zomaya, Albert και Yang, Laurence T. 2019. *Algorithms and Architectures for Parallel Processing.* Melbourne : SpringerLink, 2019.

Yılmaz, M. H. και Arslan, H. 2015. *Spoofing Attacks in Physical Layer Security, in: Local Computer Networks Conference Workshops* . s.l. : IEEE, 2015.

Zhang, K., και συν. 2014. *Sybil Attacks and their Defenses in the Internet of Things.* s.l. : IEEE, 2014.

Ma, Q., Gu, C., Hanley, N., Wang, C., Liu, W., & &. O. (22 February 2018). *A Machine Learning Attack Resistant Multi-PUF Design on FPGA.* Jeju, Korea (South): IEEE .

Marchand, C., Bossuet, L., Mureddu, U., Bochard, N., Cherkaoui, A., & Fischer, V. (Jan. 2018). *Implementation and Characterization of a Physical Unclonable Function for IoT: A Case Study With the TERO-PUF.* IEEE.

Michailidis, E. T., Kogias, D. G., & Voyiatzis, I. (2020). *A Review on Hardware Security Countermeasures for IoT:.* Egaleo, Greece.

Roelke, A., & Stan, M. R. (11-13 July 2016). *Attacking an SRAM-Based PUF through Wearout.* Pittsburgh, PA, USA: IEEE.

Tehranipoor, M., & Koushanfar, F. (2010). *A Survey of Hardware Trojan Taxonomy and Detection.* IEEE design & test of computers 27.

ΠΑΡΑΡΤΗΜΑ Α

Γενικός Κανονισμός για την Προστασία Δεδομένων

Την χρονιά 2016 και συγκεκριμένα 27 Απριλίου, θεσπίστηκε ο Κανονισμός 2016/679 (GDPR), που αφορά την προστασία των φυσικών προσώπων αναφορικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα (δεδομένα που αφορούν το υποκείμενο των δεδομένων) και την ελεύθερη κυκλοφορία των δεδομένων αυτών. Τον κανονισμό υποχρεούνται να ενσωματώσουν όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης (Ε.Ε.). Η έκδοση του Κανονισμού αυτού έφερε μία σειρά κατάργησης παλαιών νομοθεσιών, που αφορούσαν τα προσωπικά δεδομένα στα κράτη μέλη.

Α.1 GDPR ΚΑΙ IOT

Η λειτουργία του IoT περιλαμβάνει την μεταβίβαση δεδομένων μεταξύ των δικτυωμένων συσκευών του. Η συλλογή και η ανταλλαγή πληροφοριών αυξήθηκε σημαντικά με την ενσωμάτωση του IoT στις κοινωνικές δομές, δημιουργώντας νέες προκλήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα. Το IoT επεξεργάζεται σύνολα δεδομένων που τις περισσότερες φορές αφορούν αυστηρά προσωπικές πληροφορίες, αφού η τεχνολογία του έχει ενσωματωθεί σε τομείς υγείας, καθώς και σε συστήματα παρακολούθησης. Οι αυστηρά προσωπικές πληροφορίες είναι ευαίσθητα προσωπικά δεδομένα, των οποίων η διαρροή ταυτοποιεί το υποκείμενο των δεδομένων και τείνει να το βλάψει σε προσωπικό επίπεδο. Η ανάπτυξη της τεχνολογίας επέτρεψε σε δημόσιες αρχές και σε ιδιωτικές επιχειρήσεις να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτοφανή κλίμακα για την επιδίωξη των δραστηριοτήτων τους. Τα υποκείμενα των δεδομένων όλο και περισσότερο δημοσιοποιούν ακούσια και εκούσια προσωπικές πληροφορίες καθιστώντας τες διαθέσιμες σε παγκόσμιο επίπεδο. Έχοντας επίγνωση του γεγονότος, κατασκευαστικές εταιρείες συσκευών και πλατφόρμων δικτύωσης στα πλαίσια του IoT, οφείλουν να εναρμονίζονται με τον κανονισμό GDPR. Στα πλαίσια του IoT η

συγκατάθεση, όσον αφορά τα δεδομένα που επεξεργάζεται, οφείλει να εκφράζεται με τρόπο σαφή ώστε το υποκείμενο των δεδομένων[60] να έχει επίγνωση σχετικά με τα δεδομένα και τις πληροφορίες που το αφορούν άμεσα. Από πλευράς συστήματος η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται με νόμιμο τρόπο που χαρακτηρίζεται από διακριτικότητα, και να προστατεύονται από αυστηρούς μηχανισμούς ασφαλείας. Την ευθύνη για την ασφάλεια των προσωπικών δεδομένων την έχει ο υπεύθυνος της επεξεργασίας τους. Κατά συνέπεια, τυχόντα σφάλματα στα δεδομένα ή επιθέσεις που τείνουν να τα βλάψουν ως προς την ιδιωτικότητα και την ακεραιότητα τους αποτελούν βασική μέριμνα κατασκευαστικών εταιρειών.

[60] Το άτομο που αφορούν τα δεδομένα

ΠΑΡΑΡΤΗΜΑ Β

ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΤΩΝ ΠΡΑΓΜΑΤΩΝ

Η τεχνολογία του IoT οφείλει να «ακολουθεί» βασικές αρχές. Προκειμένου να μπορεί να χαρακτηριστεί ασφαλές ως προς την χρήση του το IoT, καθένα από τα επίπεδα του, πρέπει να προστατεύει το απόρρητο των δεδομένων που μεταβιβάζονται. Η ευκολία διασύνδεσης «έξυπνων» και διάφορων τύπων συσκευών στα συστήματα IoT «θίγει» βασικά ζητήματα ασφαλείας. (Genc, et al., 2015).

Β.1 Εμπιστευτικότητα

Η προστασία των προσωπικών δεδομένων αποτελεί πυλώνα στα πλαίσια σχεδιασμού της ασφάλειας ενός συστήματος IoT. Η εμπιστευτικότητα συντελεί μία βασική αρχή ασφαλείας που σχετίζεται άμεσα με τα δεδομένα. Το IoT είναι δυνητικά μια τεράστια και μαζική πηγή δεδομένων, συχνά και προσωπικών δεδομένων, χαρακτηριστικό που αυξάνει την απαίτηση ως προς την εμπιστευτικότητα τους. Σε πολλές περιπτώσεις, τα δεδομένα και οι πληροφορίες που διακινούνται αποτελούν και ευαίσθητα δεδομένα, δηλαδή δεδομένα που προσωποποιούν τους χρήστες και η τυχόν διαρροή τους αντικρούεται με τον κανονισμό περί προστασίας προσωπικών δεδομένων GDPR (Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων) (βλ. αναλυτικά Παράρτημα Α). Στόχος της αρχής της εμπιστευτικότητας είναι η διασφάλιση του απορρήτου και η προστασία ευαίσθητων πληροφοριών. Η απαίτηση της εμπιστευτικότητας διασφαλίζεται από μηχανισμούς εξουσιοδοτημένης πρόσβασης. Η εξουσιοδοτημένη πρόσβαση ως μηχανισμός, εξασφαλίζει ότι οι

πληροφορίες που συλλέγονται από τις συσκευές του IoT θα πρέπει να μεταδίδονται μόνο σε εξουσιοδοτημένες οντότητες.

Εκτός της εξουσιοδοτημένης πρόσβασης που είναι θεμέλιο για την διασφάλιση της εμπιστευτικότητας των δεδομένων, εξίσου σημαντικός μηχανισμός που μπορεί να συνεισφέρει στην διατήρηση της απαίτησης αυτής είναι η επαλήθευση σε δύο βήματα. Κατά την επαλήθευση σε δύο βήματα ο χρήστης έχει την δυνατότητα να αποκτά πρόσβαση στα δεδομένα με την προϋπόθεση να έχει περάσει δύο εξαρτημένες δοκιμές ελέγχου ταυτότητας [50]. (Miorandi, et al., 2012).

B.2 Ακεραιότητα

Η ακεραιότητα είναι μία σημαντική απαίτηση ασφαλείας του IoT και σχετίζεται με τις πληροφορίες και τα προσωπικά δεδομένα. Κυβερνοεγκληματίες έχουν την τάση να θέτουν σε κίνδυνο τα δεδομένα ως προς την ακεραιότητα τους στα συστήματα IoT. Η ακεραιότητα διασφαλίζει ότι ληφθέντα δεδομένα δεν έχουν μεταβληθεί και τροποποιηθεί κατά τη διακίνηση τους από οντότητα σε οντότητα. Μέθοδοι που μπορούν να συνδράμουν στην απαίτηση για ακεραιότητα των δεδομένων είναι ο έλεγχος κυκλικού πλεονασμού (CRC) και ο έλεγχος έκδοσης. Ο μηχανισμός ελέγχου κυκλικού πλεονασμού, λειτουργικά, προσθέτει μια τιμή ελέγχου σταθερού μήκους για την ανίχνευση τυχόν σφαλμάτων στην επικοινωνία μέσω διαδικτύου, μεταξύ των οντοτήτων στο IoT. Ο έλεγχος έκδοσης δημιουργεί αντίγραφα ασφαλείας των δεδομένων για να διατηρήσει τυχόν αλλαγές αρχείων στο σύστημα. Ο δεύτερος εκ των παραπάνω μηχανισμών, λειτουργεί αντικρουόμενα στην περίπτωση που επιτιθέμενος κατορθώσει να διαγράψει τα δεδομένα [49]. (Atzori, et al., 2010)

Β.3 Διαθεσιμότητα

Η διαθεσιμότητα συντελεί μία εξίσου βασική αρχή, η οποία είναι απαραίτητη στα πλαίσια της ασφάλειας του συστήματος IoT. Ο όρος «διαθεσιμότητα» συνδέεται με την διασφάλιση της δυνατότητας «επιβίωσης» των υπηρεσιών IoT σε εξουσιοδοτημένα μέρη παρά τις επιθέσεις άρνησης. Σχετικές επιθέσεις που τείνουν να βλάψουν την αδιάλειπτη ροή των δεδομένων αποτελούν οι επιθέσεις άρνησης εξυπηρέτησης (DoS) και οι επιθέσεις κατανεμημένης άρνησης εξυπηρέτησης (DDoS). Η αρχή της διαθεσιμότητας εξασφαλίζει, επίσης, ότι υπάρχει η δυνατότητα παροχής ελάχιστου επίπεδου υπηρεσιών παρά την παρουσία απώλειας ισχύος. Σημαντικό μέτρο άμυνας σε επιθέσεις άρνησης για την υποστήριξη της διαθεσιμότητας των δεδομένων, αποτελεί ο μηχανισμός φιλτραρίσματος του δρομολογητή.

Β.4 Ιδιωτικότητα

Η ιδιωτικότητα είναι μία εξίσου βασική απαίτηση που σχετίζεται άμεσα με το σύνολο των δεδομένων και των πληροφοριών. Το απόρρητο των διαθέσιμων και αποθηκευμένων πληροφοριών πρέπει αυστηρώς να διατηρείται. Ένα δίκτυο IoT, δεν πρέπει να αποκαλύπτει τις τιμές των αισθητήρων σε γειτονικές οντότητες. Η αποκάλυψη πληροφοριών θα «θίξει» το θέμα της ιδιωτικότητα των δεδομένων, γεγονός που ενδέχεται να αποτελέσει διαρροή ακόμα και ευαίσθητων προσωπικών δεδομένων. Η ιδιωτικότητα σχετίζεται άμεσα με την προστασία των πληροφοριών σε εγκεκριμένο κόμβο IoT και στην αποτροπή πρόσβασης σε αυτόν ή ακόμα και με την αποτροπή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένες οντότητες. Για την εξασφάλιση της ιδιωτικότητας, το αντίμετρα που προτείνονται είναι η χρήση τεχνικών στις ροές πληροφοριών (Flow Control), οι οποίες προσδίδουν τη δυνατότητα στα μεταδιδόμενα δεδομένα να χαρακτηρίζονται ως προς την αιτία μεταφοράς τους. Επιπρόσθετα, η εξασφάλιση της ανωνυμίας μπορεί να συνδράμει στην διατήρηση της ιδιωτικότητας των πληροφοριών. Η υποστήριξη της ανωνυμίας παρέχει την δυνατότητα απόκρυψης της πηγής των δεδομένων συμβάλλοντας στην διατήρηση του απορρήτου των δεδομένων.

Β.5 Ανθεκτικότητα και Ευστάθεια

Τα συστήματα IoT αποτελούν όλο ένα και περισσότερο στόχο «τρίτων», οι οποίοι πολλές φορές επιδιώκουν την παραβίαση και την πρόκληση διαταραχών. Βασική απαίτηση των συστημάτων είναι η ανθεκτικότητα και η ευστάθεια. Η ανθεκτικότητα σχετίζεται με την προστασία συστήματος και την ανταπόκριση του, παρά τυχόν διαταραχές που ενδέχεται να δημιουργήσουν οι επιτιθέμενοι. Εάν ένα σύστημα χαρακτηρίζεται από ανθεκτικότητα σημαίνει ότι επιστρέφει υπηρεσίες ανεξαρτήτως κακόβουλων δραστηριοτήτων που ταράζουν το σύστημα. Ο όρος «ευστάθεια» σε συνδυασμό με την ανθεκτικότητα προσθέτει την δυνατότητα αντίστασης του συστήματος σε επιθέσεις και εξωτερικές διαταραχές χωρίς να υπάρχει ανάγκη αλλαγής της υπηρεσίας του συστήματος IoT.

Β.6 Αξιοπιστία

Η ύπαρξη των βασικών απαιτήσεων της εμπιστευτικότητας και της ακεραιότητας συνδράμουν στην αξιοπιστία των συστημάτων σχετικά με τα δεδομένα. Ο όγκος των πληροφοριών και των δεδομένων που μεταβιβάζονται κατά την επικοινωνία οφείλουν να χαρακτηρίζονται από την αρχή της αξιοπιστίας. Η απαίτηση της αξιοπιστίας εξασφαλίζει ότι τα δεδομένα διακρίνονται από ορθότητα. Η ορθότητα των πληροφοριών σε συνδυασμό με την σωστή μετάδοση τους καλύπτουν την απαίτηση της αξιοπιστίας στα συστήματα IoT.

Β.7 Έλεγχος πρόσβασης – έλεγχος ταυτότητας - εξουσιοδότηση

Βασικοί μηχανισμοί ασφαλείας ως προς το επίπεδο πρόσβασης στο IoT, συναποτελούν: ο έλεγχος ταυτότητας, ο έλεγχος πρόσβασης και η εξουσιοδότηση. Αναλυτικότερα, ο έλεγχος πρόσβασης διασφαλίζει την πρόσβαση μόνο εξουσιοδοτημένων οντοτήτων σε εγκεκριμένους πιστοποιημένους κόμβους στα συστήματα IoT. Ο έλεγχος ταυτότητας είναι μία λειτουργία ιδιαίτερα σημαντική για την ασφάλεια του. Η αυξανόμενη σύνδεση συσκευών στο διαδίκτυο αποτελεί γεγονός

εκμετάλλευσης για κακόβουλους χρήστες. Για την εξασφάλιση της ταυτότητας της συσκευής, η οποία θα διαμοιραστεί δεδομένα, απαιτείται έλεγχος ταυτότητας. Με τον ορθό έλεγχο ταυτότητας ο δέκτης των πληροφοριών επαληθεύει εάν τα ληφθέντα δεδομένα προέρχονται από τη σωστή πηγή. Ουσιαστικά, μία συσκευή με τον έλεγχο ταυτότητας διασφαλίζει την ταυτότητα της οντότητας που επικοινωνεί (ανταλλάζει δεδομένα). Η εξουσιοδότηση αποτελεί επίσης, έναν βασικό μηχανισμό ασφαλείας των συστημάτων IoT στο επίπεδο πρόσβασης. Πληρώντας αυτή τη λειτουργία το σύστημα, κατά τον σχεδιασμό της ασφαλείας του, εξασφαλίζεται ότι οι υπηρεσίες και οι πόροι του δικτύου εξυπηρετούν μόνο εξουσιοδοτημένες συσκευές. Έτσι, δυσκολεύει το έργο των επιτιθέμενων, αφού ως μη εξουσιοδοτούμενοι δεν μπορούν «ξεγελάσουν» εύκολα τον μηχανισμό και να έχουν πρόσβαση σε πόρους και υπηρεσίες [82]. (Genc, et al., 2015).

ΠΑΡΑΡΤΗΜΑ Γ

Ο παρακάτω πίνακας παρουσιάζει εν συντομία τις βασικές απαιτήσεις ασφαλείας κάθε επιπέδου της αρχιτεκτονικής του IoT.

Επίπεδα IoT	Απαιτήσεις ασφαλείας
Επίπεδο Εφαρμογών	❖ Ελαχιστοποίηση όγκου δεδομένων για συγκεκριμένη εφαρμογή. ❖ Προστασία απορρήτου και διαχείριση πολιτικής. ❖ Αυθεντικοποίηση. ❖ Εξουσιοδότηση και Διαβεβαίωση ταυτότητας ❖ Κρυπτογράφηση συγκεκριμένης εφαρμογής και κρυπτογραφία στα πλαίσια των εφαρμογών.
Επίπεδο Υπηρεσιών	❖ Προστασία στην διαχείριση των δεδομένων και των πληροφοριών. ❖ Αποθήκευση κρυπτογραφικών δεδομένων σε ασφαλή βάση. ❖ Ασφαλή επεξεργασία των δεδομένων εντός δικτύου, ασφαλής υπολογισμός,

	ασφαλή συγκέντρωση των δεδομένων αυτών και παροχή ασφαλούς υπολογιστικού νέφους (cloud).
Επίπεδο Δικτύου	❖ Ασφαλής αλληλεπίδραση αισθητήρα με cloud. ❖ Ασφάλεια κατά την διαχείριση των δεδομένων μεταξύ όλων των επιπέδων της αρχιτεκτονικής του IoT. ❖ Ασφάλεια κατά την επικοινωνία και την συνδεσιμότητα των «πραγμάτων».
Επίπεδο Ανίχνευσης	❖ Έλεγχος πρόσβασης σε κόμβους ❖ Ελαφριά σε ισχύ κρυπτογράφηση ❖ Μορφή δεδομένων και δομές ❖ Έμπιστες οντότητες και βεβαίωση ταυτότητας τους.

Πίνακας 8: Απαιτήσεις ασφαλείας στα επίπεδα της αρχιτεκτονικής του IoT[61] [86]. (Pate, et al., 2016)

[61] https://www.semanticscholar.org/