Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνίων

Τμήμα Ψηφιακών Συστημάτων

Προπτυχιακό Πρόγραμμα Σπουδών

Ομαδική Εργασία εξαμήνου

Προστασία της Ιδιωτικότητας στο Διαδίκτυο των Πραγμάτων

Privacy in the Internet of Things

Επιβλέπων Καθηγητής: Κωνσταντίνος Λαμπρινουδάκης

Πειραιάς

Ιούνιος 2024

Στοιχεία Ομάδας

	Ονοματεπώνυμο	ΑΜ	e-mail
1	Παναγιώτης Παπακωνσταντίνου	E21135	panagiotis20035@gmail.com
2	Ειρήνη Λώλη	E21092	irini.loli@outlook.com
3	Γιώργος Τσιτσίρης	E21179	giotsi909@gmail.com

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε τον καθηγητή Κωνσταντίνο Λαμπρινουδάκη για την καθοδήγηση και την υποστήριξή του κατά τη διάρκεια του μαθήματος "Τεχνολογίες Διασφάλισης Ιδιωτικότητας". Οι γνώσεις που μας μετέδωσε θα μας βοηθήσουν πολύ στη μελλοντική μας πορεία.

Επίσης, θα θέλαμε να ευχαριστήσουμε τα μέλη της ομάδας μας για την άριστη συνεργασία και την αφοσίωσή τους στην εκπόνηση αυτής της εργασίας. Η συνεργασία και η αμοιβαία υποστήριξή μας βοήθησαν να επιτύχουμε κάτι που μας ενέπνευσε και μας έκανε υπερήφανους.

Abstract

In recent years, the protection of personal data faces ongoing challenges due to the insufficiently defined legislative framework for privacy, influenced by the constantly changing landscape and needs. In the Internet of Things (IoT), there is insecurity in terms of privacy, as organisations often lack sufficient knowledge and do not implement adequate security mechanisms, thereby violating users' rights.

Consumers must be well-informed about the information they share and its potential impacts, while manufacturers need to enforce stricter security standards and demonstrate greater transparency in their practices. Because of the massive number of interconnected devices available today, data and physical security becomes necessary. Also, access control schemes are required to avoid loss of data.

This review deepens the complexities of privacy in IoT by considering the current regulatory landscape, compliance challenges and effective methods for ensuring privacy in IoT ecosystems. By highlighting the best practices and recommending strategies for enhanced security, we aim to contribute to the development of a more secure and privacy-conscious IoT environment in the future.

Εννοιολογικό πλαίσιο

Internet of Things (IoT): Δίκτυο ευρείας ποικιλίας συνδεδεμένων συσκευών, το οποίο εξυπηρετεί την επικοινωνία μεταξύ των συσκευών αυτών και των υπηρεσιών Cloud και Διαδικτύου.

Έξυπνα σπίτια (Smart Homes): Τεχνολογία για αυτοματοποιημένη διαχείριση και έλεγχο εγκαταστάσεων σπιτιού.

Έξυπνες πόλεις (Smart Cities): Χρήση τεχνολογίας για βελτίωση της αστικής ζωής και των υποδομών.

Έξυπνη υγεία (Smart Health): Καινοτόμες τεχνολογίες για βελτίωση της παροχής υγειονομικής περίθαλψης.

Επίθεση άρνησης εξυπηρέτησης ("distributed" denial of service attacks, DoS, DDoS): Είδη και επιθέσεις στο διαδίκτυο για αποτροπή ή διακοπή υπηρεσιών.

Elliptic Curve: Μαθηματική καμπύλη χρησιμοποιούμενη στην κρυπτογραφία.

Κρυπτογράφηση: Προστασία δεδομένων με μαθηματικούς αλγορίθμους.

Lightweight Κρυπτογράφηση: Είδος κρυπτογραφικού αλγορίθμου για χρήση σε συσκευές με ελάχιστους υπολογιστικούς πόρους

Διεθνής Οργανισμός Τυποποίησης (ISO): Διεθνής οργανισμός για τυποποίηση προτύπων.

Έλεγχος πρόσβασης στο δίκτυο (Network Access Control (NAC)): Τεχνολογία για τον έλεγχο και τη διαχείριση πρόσβασης σε δίκτυα.

Έξυπνα αντικείμενα (smart objects): Συσκευές που συνδέονται στο διαδίκτυο για αυτοματισμό και διαχείριση.

Blockchain: Τεχνολογία κατανεμημένου καθολικού καταμερισμού για ασφαλή και αξιόπιστη αποθήκευση και διαχείριση δεδομένων.

Διακομιστής (Server): Υπολογιστικό σύστημα που παρέχει υπηρεσίες ή δεδομένα σε άλλους υπολογιστές μέσω δικτύου.

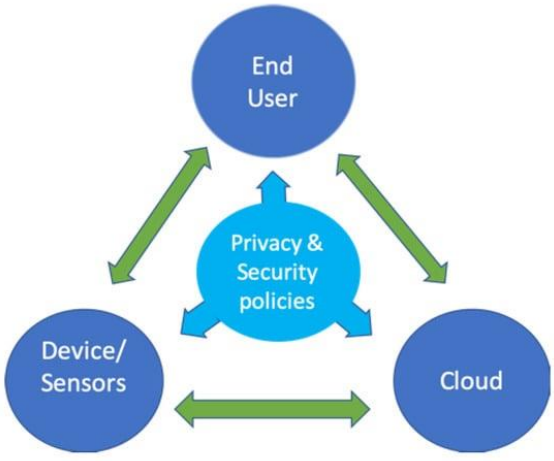
Περιεχόμενα

1. Εισαγωγή στο Διαδίκτυο των πραγμάτων (IoT)

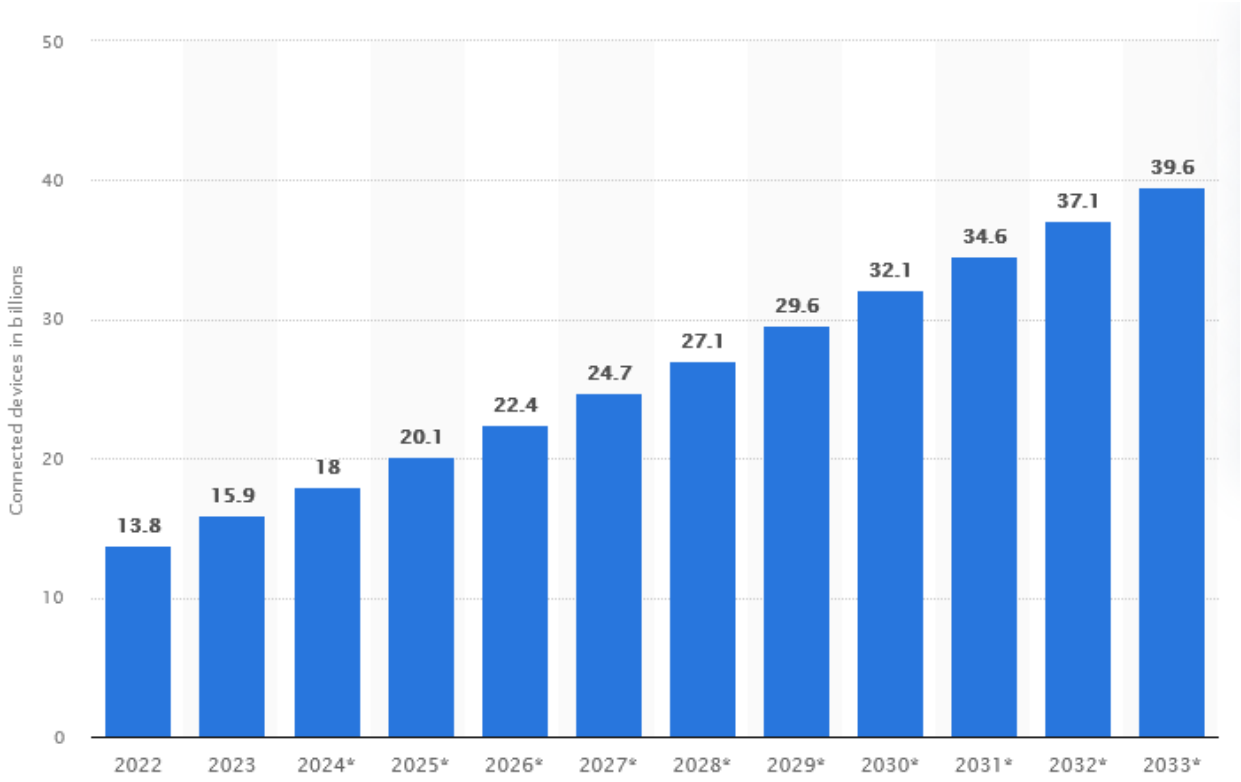
Η ταχύτατη εξάπλωση του Διαδικτύου των Πραγμάτων (IoT) έχει φέρει μεγάλη αλλαγή στον τρόπο που χρησιμοποιούνται οι συσκευές, σε διάφορες εφαρμογές και για πολλούς σκοπούς. Με την χρήση συσκευών IoT βελτιώνεται η αποδοτικότητα πολλών διαδικασιών σε πολλούς κοινωνικούς και βιομηχανικούς τομείς κάνοντας την καθημερινή μας ζωή ευκολότερη. Όμως, οι συσκευές αυτές συλλέγουν, μεταφέρουν και επεξεργάζονται μεγάλο όγκο δεδομένων, τα οποία αφορούν προσωπικές προτιμήσεις, συνήθειες και καθημερινές δραστηριότητες, δεδομένα τοποθεσίας, βιομετρικά δεδομένα και πληροφορίες για την υγεία.

Πώς, λοιπόν, μπορεί η αυξημένη συλλογή, ανάλυση και χρήση δεδομένων από τις συσκευές του Διαδικτύου των Πραγμάτων να επηρεάσει την ιδιωτικότητα των χρηστών και ποια είναι τα κύρια μέτρα που μπορούν να ληφθούν για την εξασφάλιση της ιδιωτικότητας σε αυτό το πλαίσιο;

Αυτό, δημιουργεί απαιτήσεις για τους οργανισμούς που χρησιμοποιούν τέτοιες συσκευές να πάρουν τα κατάλληλα μέτρα για την προστασία της ακεραιότητα και της εμπιστευτικότητας των δεδομένων τους και ταυτόχρονα να διασφαλίζουν την ιδιωτικότητα των υποκειμένων από τα οποία συλλέγουν οποιαδήποτε πληροφορία. Για αυτόν τον λόγο, δημιουργούνται και εξελίσσονται συνεχώς κανονισμοί από αρχές, όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR - 2016/679) της Ευρωπαϊκής Ένωσης, που επιβάλλουν κανονισμούς στις επιχειρήσεις και οργανισμούς σε σχέση με την προστασία των προσωπικών δεδομένων που έχουν στην κατοχή τους. Υπάρχουν πολλοί τρόποι για να προστατευθούν τα δεδομένα, συνήθως όμως χρησιμοποιούνται μέθοδοι που έχουν αποδειχθεί αποδοτικοί από παγκόσμιους οργανισμούς προτυποποίησης, όπως ο ISO και ο NIST. Αυτοί περιλαμβάνουν αλγόριθμους κρυπτογράφησης και τεχνικές για την ασφαλή αποθήκευση και μεταφορά των δεδομένων, αλλά και μεθόδους για την πραγματοποίηση ελέγχου προσπέλασης ώστε να μην αποκτήσουν πρόσβαση μη-επιθυμητοί χρήστες στο σύστημα.



Γενικό μοντέλο για την προστασία των Internet of Things (IoT) με πολιτικές ιδιωτικότητας. www.mdpi.com/2076-3417/10/12/4102



Αριθμός συνδέσεων Internet of Things (IoT) παγκοσμίως από το 2022 έως το 2023, με προβλέψεις από το 2024 έως το 2033 https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

2. Κανονιστικές Αρχές και Απαιτήσεις του ΓΚΠΔ

Το Διαδίκτυο των πραγμάτων (IoT) είναι βασισμένο σε ένα μεγάλο πλήθος αισθητήρων συνδυασμένο με λογισμικό, με σκοπό να παραχθούν και να ανταλλαχθούν δεδομένα μέσω του διαδικτύου. Το πλήθος των συσκευών και η ικανότητά τους να λειτουργούν χωρίς διακοπή τους δίνει τη δυνατότητα να παράγουν τεράστιο όγκο δεδομένων, ο οποίος συλλέγεται και επεξεργάζεται. Στην σημερινή εποχή όπου η πληροφορία θεωρείται πολύτιμη, η ελεύθερη συλλογή της πληροφορίας απο τις IoT συσκευές θεωρείται απειλή και πρέπει να περιοριστεί με σκοπό την ασφάλεια και την ιδιωτικότητα του κοινού.

2.1 Συγκατάθεση

Οι συσκευές IoT έχουν πολλές προκλήσεις όσον αφορά την ιδιωτικότητα. Μία από αυτές είναι η συγκατάθεση. Η «συγκατάθεση» ορίζεται από το άρθρο 4 του GDPR ως «κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν

αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν»[1] . Όλες οι συσκευές IoT είναι αυτοματοποιημένες και βασίζονται στην απουσία χειριστή, πράγμα που καθιστά αδύνατο να υπάρξει κάποια συγκατάθεση από τον χρήστη. Από την άλλη, η επικοινωνία μεταξύ των συσκευών (M2M), δημιουργεί προβληματισμούς στην ιδιωτικότητα καθώς δεν μπορεί να ελεγχθεί με ακρίβεια η επεξεργασία και μεταφορά των πληροφοριών. Επιπλέον, δεν μπορεί να οριστεί υπεύθυνος επεξεργασίας λόγω του ότι οι συσκευές συλλέγουν, επεξεργάζονται αυτόνομα. Επομένως, καταλήγουμε στο συμπέρασμα ότι οι ισχύοντες κανόνες του ΓΚΠΔ δεν μπορούν να εφαρμοστούν στο IoT, δημιουργώντας υψηλό κίνδυνο όσον αφορά την ασφάλεια και την προστασία της ιδιωτιωτικότητας.

2.2 Διαφανής Επεξεργασία

Ένα ακόμη πρόβλημα που συναντάμε στον κόσμο του IoT είναι η διαφανής επεξεργασία. Το ΓΚΠΔ αναφέρεται ξεκάθαρα στη διαφανή επεξεργασία στο άρθρο 5 (1α) « Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία κατά τρόπο νόμιμο, δίκαιο και διαφανή σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αμεροληψία και διαφάνεια»), » [2]. Η συλλογή, η αποθήκευση και η ανάλυση των πληροφοριών πραγματοποιούνται σε μεγάλη έκταση, καθιστώντας αρκετά πολύπλοκη τη διασφάλιση της διαφανούς επεξεργασίας. Ο έλεγχος των πληροφοριών είναι αρκετά σύνθετος, καθώς τα δεδομένα μεταπηδούν από συσκευή σε συσκευή (IoT), δημιουργώντας πολλά προβλήματα στη μεταφορά και την αποθήκευση. Επιπρόσθετα, δεν υπάρχουν συστήματα που να παρέχουν στον χρήστη πλήρη πρόσβαση και έλεγχο όλων αυτών των πληροφοριών αλλά ούτε και για να ελέγχουν την επεξεργασία τους. Με άλλα λόγια, δεν υπάρχει αμεσότητα μεταξύ του χρήστη και των διαδικασιών, διότι ο χρήστης δεν μπορεί να συναινέσει, δεν μπορεί να γνωρίζει ποια δεδομένα συλλέγονται και επεξεργάζονται, δεν μπορεί να τα τροποποιήσει, καθώς και δεν γνωρίζει πού και ποιος έχει πρόσβαση στα δεδομένα του. Έτσι, δημιουργούνται σημαντικά ζητήματα ασφάλειας και ιδιωτικότητας, αφού οι χρήστες δεν μεριμνούν επαρκώς για τα προσωπικά τους δεδομένα. Για αυτό τον λόγο, είναι μείζον ζήτημα να αναπτυχθούν καινοτόμοι μηχανισμοί όπου θα εφαρμόζουν την διαφανή επεξεργασία ώστε να διασφαλιστεί η προστασία και ιδιωτικότητα των δεδομένων.

2.3 Ελαχιστοποίηση Δεδομένων

Η Ελαχιστοποίηση Δεδομένων είναι και αυτή εξίσου σημαντική. Αναφέρεται στο ΓΚΠΔ ως «Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκείς, συναφείς και περιορισμένα στο αναγκαίο μέτρο σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία».[3]

Οι συσκεύες IoT συλλέγουν και επεξεργάζονται συνεχώς δεδομένα προσφέροντας υπηρεσίες στον χρήστη, όμως για να συμμορφωθούν στον κανονισμό θα πρέπει να συλλέγουν μόνο τα δεδομένα που είναι απολύτως απαραίτητα για τη λειτουργία της συσκευής. Ακόμα, τα δεδομένα που συλλέγονται πρέπει να υποβάλλονται σε επεξεργασία μόνο για τον σκοπό που έχουν αρχικά

συλλεχθεί και όχι για άλλους σκοπούς. Για παράδειγμα, ένας έξυπνος οικιακός βοηθός όπου συλλέγει δεδομένα φωνής για να εκτελεί εντολές του χρήστη, θα πρέπει να επεξεργάζεται και να συλλέγει μόνο ηχητικά που σχετίζονται με τις φωνητικές εντολές και να τα διαγράφει μετά από εύλογο χρονικό διάστημα. Η Ελαχιστοποίηση των δεδομένων στο Διαδίκτυο των πραγμάτων συνδράμει στην προστασία της ιδιωτικότητας, μειώνει τον κίνδυνο και ενισχύει την εμπιστοσύνη των χρηστών προς τις συσκευές.

2.4 Δικαίωμα στη Λήθη

Το δικαίωμα στη λήθη αποτελεί ένα κρίσιμο ζήτημα στο Διαδίκτυο των Πραγμάτων (IoT). Αυτό το δικαίωμα παρέχει στους χρήστες τη δυνατότητα να αιτούνται τη διαγραφή των δεδομένων τους οποιαδήποτε στιγμή, με σκοπό την εξασφάλιση της ιδιωτικότητάς τους. Ωστόσο, στον κόσμο του IoT, αυτό καθίσταται εξαιρετικά περίπλοκο λόγω της συνεχούς μεταφοράς των πληροφοριών και της αποθήκευσής τους σε πολλές συσκευές και βάσεις δεδομένων. Παρά το γεγονός ότι οι ισχύοντες κανονισμοί της Ευρωπαϊκής Ένωσης[4] και των επιμέρους κρατών αναγνωρίζουν το δικαίωμα στη λήθη ως θεμελιώδες δικαίωμα των χρηστών, δεν παρέχουν σαφείς οδηγίες για την εφαρμογή του στον κόσμο του IoT. Αυτό έχει ως αποτέλεσμα την ανεπαρκή παροχή του δικαιώματος στη λήθη, καθώς και την έλλειψη συστημάτων που θα διασφαλίζουν την αποτελεσματική εφαρμογή του. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί την ανάπτυξη νέων τεχνολογικών λύσεων και νομοθετικών ρυθμίσεων που θα λαμβάνουν υπόψη τις ιδιαιτερότητες του IoT, διασφαλίζοντας έτσι την προστασία της ιδιωτικότητας των χρηστών.

2.5 Δικαιώματα πρόσβασης, διόρθωσης και φορητότητας

Τα Δικαιώματα πρόσβασης, διόρθωσης και φορητότητας είναι ζωτικής σημασίας στο πλαίσιο της διακυβέρνησης των δεδομένων του Διαδικτύου των πραγμάτων (IoT). Το δικαίωμα πρόσβασης επιτρέπει στα άτομα να έχουν γνώση των προσωπικών τους δεδομένων, συμπεριλαμβανομένων των πληροφοριών σχετικά με το τι συλλέγεται, αν αυτά επεξεργάζονται, τους σκοπούς της επεξεργασίας και τους αποδέκτες των δεδομένων[5]. Το δικαίωμα διόρθωσης επιτρέπει στα άτομα να διορθώνουν ανακριβή δεδομένα ή να προσθέτουν επιπλέον πληροφορίες[6]. Το δικαίωμα στη φορητότητα επιτρέπει στα άτομα να μεταφέρουν τα δεδομένα τους σε άλλον πάροχο υπηρεσιών IoT[7]. Ωστόσο, η πολυπλοκότητα και ο μεγάλος όγκος των δεδομένων καθιστούν δύσκολη τη συμμόρφωση των οργανισμών με αυτές τις απαιτήσεις. Επιπλέον, δεν υπάρχει κάποιος καθιερωμένος τρόπος για τη μεταφορά δεδομένων ανάμεσα σε εταιρίες IoT, γεγονός που περιπλέκει ακόμα περισσότερο τη διαδικασία. Οι οργανισμοί πρέπει να διαθέσουν σημαντικούς πόρους και χρήματα για να διασφαλίσουν τη λειτουργικότητα αυτών των δικαιωμάτων, κάτι που συχνά παραμελείται. Οι προβληματισμοί αυτοί αναδεικνύουν την ανάγκη για πιο αποδοτικές υποδομές και τεχνολογίες διαχείρισης δεδομένων, έτσι ώστε να

εφαρμόζονται στην πράξη τα δικαιώματα των ατόμων και να εξασφαλίζεται η ασφάλεια και η ιδιωτικότητα των δεδομένων.

2.6 Αρχή της Λογοδοσίας

Η αρχή της λογοδοσίας στον ΓΚΠΔ απαιτεί από τους υπευθύνους επεξεργασίας δεδομένων να αποδεικνύουν ότι συμμορφώνονται με τον κανονισμό και να εφαρμόζουν πολιτικές και μηχανισμούς προστασίας δεδομένων για τη χρήση δεδομένων σε συσκευές IoT. Η αρχή της λογοδοσίας αναφέρεται κυρίως στα άρθρα 5(2)[8], 24[9] και 28(3)[10] του ΓΚΠΔ. Για τις συσκευές IoT, η υποχρέωση απόδειξης της συμμόρφωσης με τον κανονισμό απαιτεί την υλοποίηση ειδικών μέτρων, συμπεριλαμβανομένης της ανάπτυξης ασφαλών προϊόντων [11]. Οι διατάξεις αυτές συντελούν στη διασφάλιση της προστασίας των δεδομένων και στην λογοδοσία των οργανισμών που αναπτύσσουν συσκευές IoT, προάγοντας έτσι την εμπιστοσύνη μεταξύ των χρηστών.

2.7 Ψευδωνυμοποίηση

Η ψευδωνυμοποίηση παίζει κρίσιμο ρόλο στην διασφάλιση των προσωπικών δεδομένων. Ορίζεται στο άρθρο 4(5) του ΓΚΠΔ και αναφέρεται ως «η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο δεδομένων χωρίς τη χρήση πρόσθετων πληροφοριών, υπό την προϋπόθεση ότι αυτές οι πρόσθετες πληροφορίες τηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα για να διασφαλιστεί ότι τα προσωπικά δεδομένα δεν αποδίδονται σε αναγνωρισμένο ή αναγνωρίσιμο φυσικό πρόσωπο»[12].

Δεδομένου ότι τα δεδομένα στις συσκευές IoT αποθηκεύονται σε βάσεις δεδομένων και διαμοιράζονται συνεχώς, η πρακτική της ψευδωνυμοποίησης μπορεί να αποτρέψει πολλές δυσάρεστες καταστάσεις όπου τα δεδομένα θα κατέληγαν σε λάθος χέρια, είτε από τρίτους παράγοντες που είναι υπεύθυνοι για την επεξεργασία είτε από επιτιθέμενους. Η ψευδωνυμοποίηση είναι ένας αποτελεσματικός τρόπος για την εφαρμογή της αρχής της ελαχιστοποίησης δεδομένων σύμφωνα με το άρθρο 5(1)(γ)[13].

Αυτή η πρακτική είναι απαραίτητο να εφαρμόζεται και να επιβάλλεται από όλους τους οργανισμούς, καθώς μόνο με αυτόν τον τρόπο θα διασφαλιστεί η ιδιωτικότητα των χρηστών.

2.8 Ιδιωτικότητα από Σχεδιασμό (Privacy by Design)

Η αρχή Privacy by Design απαιτεί απο την αρχή του κύκλου ζωής του προϊόντος να χρησιμοποιηθούν όλες οι δυνατές προστατευτικές ρυθμίσεις και αναλύεται στα άρθρα 5(1)(b) 32(1)(b) και 25(1) του ΓΚΠΔ.[14][15][16]

2.8.1 Επικοινωνία και Εκπαίδευση (Communication and Education)

Ένα από τα πιο σημαντικά μέρη του ιδιωτικότητας από σχεδιασμό αφορά το κομμάτι της εκπαίδευσης του αρμόδιου προσωπικού για τον κύκλο ζωής των IoT, αλλά και των χρηστών. Η ανάπτυξη πολιτικής επίγνωσης των κινδύνων και η εφαρμογή των πολιτικών αυτών αυξάνει την επίγνωση των κινδύνων, άρα και της αντίληψης τους. Οι χρήστες οφείλουν να ενδιαφέρονται και να ενημερώνονται για τους πιθανούς κινδύνους με τρόπο διαφανή από την πλευρά της αντίστοιχης εταιρίας, ώστε να αποφευχθούν και από τις δύο πλευρές οι επιπτώσεις. Οι πολιτικές αυτές πρέπει να ακολουθούν βασικές αρχές, όπως να είναι σύντομες, περιεκτικές και σαφείς με σκοπό την ενίσχυση της ευαισθητοποίησης των χρηστών για τις απειλές ασφάλειας στις συσκευές IoT. Τέλος, η παροχή εκπαίδευσης στους τεχνικούς και τους χρήστες σχετικά με την ασφαλή χρήση και διαχείριση των συσκευών IoT, μπορεί να γίνεται μέσω της διανομής εγχειριδίων χρήσης (manuals), τα οποία να περιέχουν αφιερωμένο κεφάλαιο για τις πρακτικές ασφαλείας των IoT συσκευών.

2.8.2 Προληπτικά Μέτρα (Preventive Measures)

Η εφαρμογή προληπτικών μέτρων στοχεύει στην αποτροπή απειλών και την προστασία ευαίσθητων δεδομένων. Τα βασικά συστατικά μέρη των μέτρων είναι:

- Η ενίσχυση της κρυπτογράφησης και της ασφάλειας δεδομένων,η προσθήκη μέτρων όπως κρυπτογράφηση για την ασφαλή επικοινωνία των συσκευών μεταξύ τους, η κατάργηση προεπιλεγμένων κωδικών πρόσβασης.
- Η εφαρμογή πολιτικών πρόσβασης μόνο σε εξουσιοδοτημένους χρήστες και επαλήθευση ταυτότητας με χρήση μεθόδων όπως πολυπαραγοντική επαλήθευση (MFA).
- Αυτόματη απομόνωση μολυσμένων συσκευών, δημιουργία μηχανισμού για την απομάκρυνση συσκευής IoT από το δίκτυο, που έχει υποστεί επεξεργασία της καθορισμένης λειτουργίας της για την αποφυγή εξάπλωσης επιθέσεων (Network Access Control (NAC) με κατάλληλο διακόπτη και ενσύρματες ενσωματώσεις).

2.8.3 Προστασία δεδομένων εξ ορισμού (By Default)

Η αρχή της προστασίας δεδομένων εξ ορισμού , όπως ορίζεται στον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) στο άρθρο 25(2)[17], διασφαλίζει ότι η σχεδίαση και η διαμόρφωση του συστήματος επεξεργασίας δεδομένων πρέπει να προσφέρουν αυτομάτως και από προεπιλογή την υψηλή προστασία των δεδομένων, χωρίς την ανάγκη ενέργειας από τον χρήστη. Η αρχή αυτή είναι απαραίτητη για να εξασφαλιστεί ότι η προστασία των δεδομένων είναι ενταγμένη στην τεχνολογική διαδικασία, προστατεύοντας έτσι τα δεδομένα, χωρίς επιπλέον ενέργειες από τον χρήστη.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων αποτελεί την θεμελιώδη βάση για την προστασία των δικαιωμάτων των χρηστών. Είναι ζωτικής σημασίας οι οργανισμοί που δραστηριοποιούνται στον τομέα του Διαδικτύου των Πραγμάτων (IoT) να εφαρμόσουν αυστηρά όλες αυτές τις πρακτικές. Μόνο μέσω της συμμόρφωσης με αυτές μπορούν να διασφαλίσουν όχι μόνο τη διαφάνεια και την ιδιωτικότητα των χρηστών, αλλά και την αποτελεσματική προστασία των προσωπικών δεδομένων.

3. Πρότυπα & Συμμόρφωση

Η διασφάλιση ότι τα προσωπικά δεδομένα κάθε χρήστη συσκευής IoT είναι ελάχιστα πιθανό να παραβιαστούν, αποτελεί πρόκληση για την εποχή όπου η ποικιλία και η ελεύθερη διακίνηση τέτοιων συσκευών και υπηρεσιών ολοένα και αυξάνεται. Προκειμένου ευρωπαϊκώς και παγκοσμίως να περιοριστούν τα ψηφιακά εγκλήματα σε IoT, επιτάσσεται η ανάπτυξη και η εφαρμογή προτύπων και κανονισμών για την ιδιωτικότητα στο IoT, αλλά και η συνεχής αναννέωσή τους, λαμβάνοντας υπόψιν τον διαμοιρασμό γνώσεων από καταγεγραμμένες νέες και παλιές, περίτεχνες πλέον απειλές στον κυβερνοχώρο (Mirai, Qbot, Kaiten). Τα πρότυπα παρέχουν στους ανθρώπους και στις επιχειρήσεις, οργανισμούς μια βάση για την αμοιβαία κατανόηση του IoT και των πτυχών που το δομούν.

3.1 Ρυθμιστικό πλαίσιο και πρότυπα (Regulatory Framework and Standards)

Οι κανονισμοί που αναφέρονται σε τεχνικές απαιτήσεις ακολουθούνται υποχρεωτικά και επιβάλλονται από κυβερνητικούς φορείς ή ρυθμιστικές αρχές, όπως ο Κανονισμός Γενικής Προστασίας Δεδομένων (GDPR) στην Ευρωπαϊκή Ένωση που αναφέρεται στο προηγούμενο κεφάλαιο. Η μη συμμόρφωση με αυτούς έχει νομικές συνέπειες, όπως πρόστιμα, κυρώσεις ή και απαγόρευση της λειτουργίας μιας επιχείρησης. [18]

Οι ρυθμιστικές αρχές και κανόνες που ορίζονται λειτουργούν υποστηρικτικά με τον ΓΚΠΔ και έχουν σκοπό να προστατέψουν χρήστες και επιχειρήσεις IoT, δημιουργώντας ένα ασφαλές περιβάλλον για τη διασύνδεσή των δυο τελευταίων, το οποίο θα είναι προστατευμένο από

κυβερνοεπιθέσεις, και θα σέβεται πάντα το ατομικό δικαίωμα για την προστασία των προσωπικών δεδομένων.

Προτού εμβαθύνουμε, είναι άξιο αναφοράς το οτι πρόσφατα δόθηκε μεγαλύτερη έμφαση στη διακήρυξη των ανθρώπινων δικαιωμάτων που αφορά την ιδιωτικότητα στο διαδίκτυο, σύμφωνα με τα άρθρα 7, 8, 12 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ [19].

Σημαντικές δράσεις της ΕΕ για ένα ρυθμιστικό πλαίσιο λειτουργίας ψηφιακών εφαρμογών στον κυβερνοχώρο είναι: η οδηγία Directive on Security of Network and Information Systems (the NIS Directive) που βελτιώνει τις δυνατότητες της κυβερνοασφάλειας και της ανθεκτικότητας των κρίσιμων υποδομών και των βασικών υπηρεσιών εντός της ΕΕ.

Χωρίζεται σε 2 οδηγίες: η πρώτη οδηγία NIS Directive 1 (Οδηγία (ΕΕ) 2016 /1148), και η δεύτερη, που προσαρμόζεται στις νέες μεταλλάξεις του κυβερνοχώρου, NIS Directive 2 (Οδηγία (EU) 2022/2555).

Κάθε ευρωπαϊκή χώρα θα πρέπει μέχρι τον Οκτώβρη του 2024 να έχει θέσει σε ισχύ την νομοθεσία για NIS Directive 2 για την κυβερνοασφάλεια των IoT και γενικότερα.
Το Ευρωπαϊκό Κοινοβούλιο υιοθέτησε επίσημα τον κανονισμό DORA - Digital Operational Resilience Act για να καθιερωθούν οι ενιαίες απαιτήσεις που διέπουν την ασφάλεια των δικτύων και των συστημάτων πληροφορικής σε ολόκληρο τον χρηματοπιστωτικό τομέα και τους τρίτους φορείς στην αλυσίδα εφοδιασμού (ΤΠΕ - Τεχνολογίες Πληροφρικής και Επικοινωνιών).

Η συμμόρφωση κατά τη δράση αυτή διασφαλίζει την ανθεκτικότητα και ανάκαμψη των οργανισμών από αναταραχές και απειλές σχετικά με τις υπηρεσίες Πληροφορικής και Επικοινωνιών (ICT - Information and Communications Technology). Περιλαμβάνει την αξιολόγηση κινδύνων, διαχείριση ευπαθειών, παρακολούθηση περιστατικών και ασφαλή απόκτηση νέων συσκευών IoT.

Η Cyber Resilience Act (CRA), προτάθηκε στην Ευρωπαϊκή Επιτροπή το 2022, επικυρώθηκε το 2023 και επίσημα θα εγκριθεί το 2024. Προβλέπει συγκεκριμένες απαιτήσεις για κατασκευαστές και εμπόρους λιανικής, για την κυβερνοασφάλεια και την ανθεκτικότητα στον κυβερνοχώρο, όπως το να αντικατασταθούν τα χαρακτηριστικά των IoT που παρουσιάζουν μη ικανοποιητικά μέτρα ασφαλείας με νέα, ισχυρότερης προστασίας.

3.1.1 Πρότυπα για το IoT

Οι ρυθμιστικές προσπάθειες αποσκοπούν στην ασφάλεια του IoT και ενισχύονται μέσω της ανάπτυξης προτύπων και κατευθυντήριων γραμμών (guidelines).

Στις Η.Π.Α., το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) έχει δημοσιεύσει οδηγίες για την κυβερνοασφάλεια του IoT, π.χ. το πρότυπο NISTIR 8425 (το οποίο ακολουθεί υποχρεωτικά τις θεμελιώδεις κατευθυντήριες γραμμές ασφάλειας Risk Management Framework - RMF και άλλες οδηγίες) εκφράζει τις απαιτήσεις ειδικά για καταναλωτικές εφαρμογές IoT

(έξυπνα ρολόγια, συσκευές έξυπνου σπιτιού, παρακολούθηση περιουσιακών στοιχείων κ.λπ.) και εφαρμόζεται στις Ηνωμένες Πολιτείες αλλά και παγκόσμια.

Το IEEE και συγκεκριμένα το IEEE P2413, είναι ένα πρότυπο που αναπτύσσεται από το IEEE (Institute of Electrical and Electronics Engineers - Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών) και στοχεύει στην παροχή ενός ολοκληρωμένου πλαισίου αρχιτεκτονικής για το IoT. Το πρότυπο αυτό βελτιώνει τη διαλειτουργικότητα, την ασφάλεια και την ιδιωτικότητα των IoT συσκευών και εφαρμογών. Προβλέπει την ενσωμάτωση ποικίλων IoT συστημάτων και την παροχή κοινών προτύπων για την ανάπτυξη ασφαλών και ανθεκτικών λύσεων για το IoT.

Το ETSI - European Telecommunications Standards Institute - Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων – επηρεάστηκε από τον Κώδικα Πρακτικής του Ηνωμένου Βασιλείου και δημοσίευσε το πρότυπο EN 303645, το οποίο προβλέπει ένα σύνολο 13 κατηγοριών συστάσεων και υιοθετείται όλο και περισσότερο παγκοσμίως [20].

Μερικές από τις διατάξεις του ETSI περιλαμβάνουν:

- Απαγόρευση των προεπιλεγμένων κωδικών πρόσβασης.
- Ανάπτυξη μέσων για τη διευκόλυνση αναφορών ευπαθειών.
- Ενημερώσεις λογισμικού.
- Ασφαλή αποθήκευση ευαίσθητων δεδομένων.
- Ασφαλή κανάλια επικοινωνίας (κρυπτογραφημένα).
- Ανθεκτικότητα των συστημάτων έναντι διακοπών λειτουργίας και ασφαλή ανάκτηση.

Η Διεθνής Ένωση Τηλεπικοινωνιών ITU (International Telecommunication Union) είναι ο εξειδικευμένος οργανισμός των Ηνωμένων Εθνών που ασχολείται με θέματα ΤΠΕ. Τα πρότυπα του ITU υιοθετούνται ευρέως και αναφέρονται παγκοσμίως, ειδικά στους τομείς των τηλεπικοινωνιών και του IoT. Το ITU-T Y.2060 ορίζει το πλαίσιο του IoT και το ITU-T Y.4806 περιγράφει το πλαίσιο ασφάλειας για το IoT, επικεντρώνοντας στην προστασία δεδομένων, στη διαχείριση ταυτότητας και στην ασφαλή επικοινωνία.

Οι CEN και CENELEC (European Committee for Standardization / European Committee for Electrotechnical Standardization) είναι Ευρωπαϊκοί οργανισμοί τυποποίησης, δημοσιεύουν εθελοντικά πρότυπα για να διασφαλίσουν την ασφάλεια, την ποιότητα και τη διαλειτουργικότητα των προϊόντων και υπηρεσιών σε όλη την Ευρώπη. Κύριες περιοχές τους περιλαμβάνουν την τυποποίηση των μετρητών αερίου (CEN/CLC/TC 13) και των τεχνολογιών αυτόματης συλλογής δεδομένων (CEN/CLC/TC 225), οι οποίες είναι κρίσιμες για την αξιοπιστία και την ασφάλεια των συστημάτων IoT.

3.1.2 Πρότυπα ISO

Το ISO/IEC 27001 :2022 είναι ένα διεθνές πρότυπο για την ασφάλεια των πληροφοριών το οποίο προδιαγράφει τις απαιτήσεις που πρέπει να πληροί ένα αποτελεσματικό Σύστημα Διαχείρισης της ασφάλειας των πληροφοριών (ΣΔΑΠ) για την εξασφάλιση των βασικών αρχών ασφάλειας: της Εμπιστευτικότητας, της Ακεραιότητας, και της Διαθεσιμότητας της πληροφορίας.

Τα βασικά στοιχεία κατά ISO/IEC 27001 περιλαμβάνουν την προστασία δεδομένων και πληροφοριών από:

- Υποκλοπή
- Πρόσβαση από μη εξουσιοδοτημένα άτομα, φορείς, τρίτους,
- Τυχαία ή εσκεμμένη αλλοίωση ή απώλεια,
- Κακόβουλες επιθέσεις μέσω του διαδικτύου, ιούς κλπ.

Από την ίδια σειρά προτύπων (ISO/IEC 27001), υπάρχει το ISO/IEC 27030, τώρα πλέον γνωστό ως ISO/IEC 27400:2022 το οποίο εστιάζει στην κυβερνοασφάλεια και την θωράκιση των προσωπικών δεδομένων για το IoT, ενσωματώνοντας τις νέες εξελίξεις στον τομέα για καλύτερη αντιμετώπιση των προκλήσεων ασφάλειας [21].

Άλλα σημαντικά πρότυπα περιλαμβάνουν το ISO/IEC 30141 για την αρχιτεκτονική IoT και το ISO/IEC 15408 για την αξιολόγηση της ασφάλειας προϊόντων IT.

Το ISO/IEC 27017 προσφέρει κατευθυντήριες γραμμές για την ασφάλεια των υπηρεσιών cloud. Αν και δεν αφορά άμεσα τις IoT συσκευές, είναι σημαντικό για τις IoT εφαρμογές που βασίζονται σε υπηρεσίες cloud, π.χ. για την αποθήκευση προσωπιών δεδομένων των χρηστών τους.

Επίσης, το ISO/IEC 27018: Εστιάζει αποκλειστικά στην προστασία προσωπικών δεδομένων στο cloud. Όπως και το ISO/IEC 27017, είναι κρίσιμο για IoT εφαρμογές που διαχειρίζονται προσωπικά δεδομένα και χρησιμοποιούν υπηρεσίες cloud.

Categorization of IoT Security Guidelines, Standards, and Regulations (Summary Table)

Name	*Type*	*Scope*	*Usage*	*Main Focus*
GDPR	Regulation	Organizations handling personal data of EU citizens	Widely applied across the EU	Protecting personal data and privacy
NIST	Standard/Guideline	Global Organizations	Widely used in the U.S. and globally	Cybersecurity guidelines for IoT
RMF	Guideline/Framework	U.S. federal agencies	Widely used in the U.S. federal sector	Managing risks to information systems
IEEE	Standard	Engineers, IoT developers, researchers	Widely used in technical communities	Framework for IoT architecture
UK Code of Practice	Guideline	IoT manufacturers in the UK	Applied in the UK	Security in consumer IoT products
GSMA	Guideline/Best Practices	Mobile network operators, IoT developers	Globally referenced	Security best practices for IoT
ETSI	Standard	Telecommunications and IoT industry in Europe	Widely used in Europe	Cybersecurity standards for IoT
NIS Directives	Regulation	EU member states, public, private sectors	Applied across the EU	Enhancing cybersecurity resilience
CRA	Regulation	Digital product manufacturers in the EU	Upcoming in the EU	Cybersecurity resilience of digital products
DORA	Regulation	Financial institutions in the EU	Applied across the EU	Operational resilience of digital systems
ENISA	Guideline/Best Practices	EU member states, public/private sectors	Referenced across the EU	Cybersecurity guidelines and support
ISO/IEC	Standard	Global organizations	Widely adopted internationally	Information security management
CEN/CENELEC	Standard	European industry sectors	Widely used in Europe	Standardization in electrotechnical and other sectors
ITU	Standard	Global telecommunications sector	Widely adopted internationally	Global standards for telecommunications and IoT

Συγκεντρωτικός Πίνακας: Κατηγοριοποίηση Κατευθυντήριων Γραμμών, Προτύπων και Κανονισμών Ασφαλείας IoT

Παρόλο που έχουν δοθεί διάφορες οδηγίες για εθελοντική συμμόρφωση με πρότυπα και συστάσεις, τείνεται κλιμακωτά να γίνουν υποχρεωτικά εφαρμόσιμες. Βασικός λόγος είναι ότι η

μη συμμόρφωση μπορεί να οδηγήσει σε αδυναμία διακίνησης συσκευών IoT σε συγκεκριμένες περιοχές, ανάλογα με τις τοπικές νομοθεσίες και κατευθυντήριες γραμμές. Δεδομένης της ποικιλομορφίας των IoT συσκευών που διασχίζουν διεθνή σύνορα, μια ενιαία προσέγγιση στην προστασία δεδομένων μπορεί να μην είναι εφικτή.

Επομένως, ο συνδυασμός εφαρμογής προτύπων, κανόνων, κανονιστικών και ρυθμιστικών πλαισίων, κρίνεται απαραίτητος για οποιαδήποτε επιχείρηση παραγωγής και διακίνησης IoT συσκευών και υπηρεσιών. Τα διεθνώς αναγνωρισμένα πρότυπα καθοδηγούν τις επιχειρήσεις στις βέλτιστες πρακτικές για την αντιμετώπιση των προκλήσεων της ασφάλειας των πληροφοριών της ίδιας και των χρηστών των IoT συσκευών, να ανταποκριθούν στις προκλήσεις της σύγχρονης ψηφιακής εποχής καθώς και να αποδείξουν την δέσμευσή τους στην ασφάλεια πληροφοριών για την ενίσχυση της εμπιστοσύνης των πελατών τους.

4. Προσεγγίσεις Μετριασμού επιπτώσεων (Mitigation Approaches)

Όλο και περισσότερες συσκευές όχι μόνο εισάγουν περισσότερες ευπάθειες ασφαλείας, αλλά επίσης αυξάνουν σημαντικά τον όγκο των δεδομένων που μεταφέρονται και πρέπει να αναλυθούν για την ανίχνευση και μετριασμό ανωμαλιών στο δίκτυο. Η ασφάλεια και η ανθεκτικότητα του περιβάλλοντος των IoT αποτελούν ένα εξαιρετικά πολύπλοκο θέμα που καλύπτει όλο τον κύκλο ζωής τους, από τον σχεδιασμό και την υλοποίηση έως την ανάπτυξη, τη λειτουργία και την απόσυρση τους. Η ανάλυση μεθόδων για την επίτευξη κάθε βήματος μετριασμού κινδύνου, εφαρμόζοντας προσεγγίσεις πολλαπλών επιπέδων ασφάλειας, μπορεί σημαντικά να καθυστερήσει την πρόοδο μιας επίθεσης στο περιβάλλον του IoT. Προκειμένου να αντιμετωπίζεται το πλήρες φάσμα πιθανών απειλών, χρειάζεται να εφαρμόζονται όλες οι προσεγγίσεις μετριασμού επιπτώσεων που αναλύονται στη συνέχεια. [22]

4.1 Αξιολόγηση και Ανάλυση Κινδύνου (Risk Assessment and Analysis)

Οι επιχειρήσεις οι οποίες παρέχουν IoT συσκεύες ή εφαρμογές στο καταναλωτικό κοινό, πρέπει να αναγνωρίζουν και να αξιολογούν τους πιθανούς κινδύνους για τυχόν ευπάθειες, όπως ανερπαρκής κρυπτογράφηση, μη ασφαλείς συνδέσεις και αδυναμία ενημέρωσης λογισμικού, για να επιτύχουν την προετοιμασία και έγκαιρη αντίδραση σε κατάσταση απειλής.

Η εκτίμηση της πιθανότητας και των επιπτώσεων των κινδύνων, όπως η διακοπή λειτουργίας IoT συσκευών σε κρίσιμες εφαρμογές, μπορεί να συμβάλλει σημαντικά στην αποτροπή διαρροής ευαίσθητων προσωπικών δεδομένων. Επίσης, η αξιολόγηση της σοβαρότητας των κινδύνων και του πιθανού αντίκτυπου, είναι σημαντικό βήμα για την κατάταξη των πιο επικίνδυνων απειλών που αντιμετωπίζονται ως πρώτες.

4.2 Στρατηγικές Αντίδρασης και Αποκατάστασης (Response and Recovery Strategies)

Η ανάπτυξη σχεδίων αντίδρασης σε κρίσιμα περιστατικά ασφαλείας, περιλαμβάνει τη ταχεία ανίχνευση προβλήματος, ταυτοποίηση του (response), απομόνωση της συσκευής και αποκατάσταση των συστημάτων που μπορεί να επηρεαστούν (recovery). Σε περίπτωση απροσδόκητης διακοπής της λειτουργίας μιας IoT συσκευής ή της εφαρμογής της, η στρατηγική εφαρμογή του πλάνου ανάκαμψης διασφαλίζει ότι το σύστημα ή η συσκευή ανακτά τη λειτουργικότητά της αυτόματα. Για την ταχεία αποκατάσταση των συστημάτων και επαναφορά τους στην κανονική τους λειτουργία, απαιτείται δέσμευση πόρων, όπως για παράδειγμα οι αποθηκευμένες ρυθμίσεις εργοστασιακών ρυθμίσεων για γρήγορη αποκατάσταση στην αρχική προγραμματισμένη λειτουργία τους.

4.3 Παρακολούθηση και Προσαρμογή (Monitoring and Adjustment)

Η συνεχής παρακολούθηση κινδύνων περιλαμβάνει την εφαρμογή αυτοματοποιημένων συστημάτων συνεχούς παρακολούθησης για την ανίχνευση αλλά και για την αντίδραση σε ασυνήθιστη συμπεριφορά συσκευών IoT σε πραγματικό χρόνο. Η προσαρμογή επίσης των στρατηγικών ασφαλείας που έχουν προοριστεί, πρέπει ενσωματώνει την υποβολή σε τακτική αναθεώρησή τους βάσει νέων απειλών (άμεσα σχετιζόμενων με την επιχείρηση ή απειλών που εντοπίζονται και δημοσιεύονται κεντρικά) και των αποτελεσμάτων της παρακολούθησης.

Αυτό σημαίνει για παράδειγμα να υπάρχουν αυτόματες ενημερώσεις και άμεσες παρεμβάσεις στις πολιτικές ασφάλειας για να αντιμετωπίζονται νέες απειλές, ενημερώντας ταυτόχρονα τους χρήστες για τις αλλαγές.

Μέσω της αναγνώρισης και αξιολόγησης των κινδύνων, της εφαρμογής προληπτικών μέτρων, και της ανάπτυξης σχεδίων αντίδρασης και ανάκαμψης, οι οργανισμοί μπορούν να βελτιώσουν σημαντικά την ασφάλεια και την ανθεκτικότητα των συστημάτων τους. Η εφαρμογή αυτών των μέτρων δεν προστατεύει μόνο τα δεδομένα και τις υποδομές, αλλά ενισχύει και την εμπιστοσύνη των χρηστών στις IoT τεχνολογίες, προάγοντας έτσι την υιοθέτηση και ανάπτυξη καινοτόμων λύσεων στον τομέα.

5. Τεχνολογίες και Μέθοδοι Διασφάλισης Ιδιωτικότητας στο IoT

Ο κύριος σκοπός των συσκευών IoT είναι η συλλογή δεδομένων από τον φυσικό περιβάλλον και η προώθησή τους στο διαδίκτυο και για αυτό τον λόγο είναι απαραίτητη η διασφάλιση τους από επιτιθέμενους λόγω της ευαίσθητης φύσης των δεδομένων που μπορεί να συλλέγονται. Για παράδειγμα, η παραβίαση συσκευών IoT ιατρικού σκοπού μπορεί να έχει μεγάλες οικονομικές επιπτώσεις αλλά και απώλειες ανθρώπινης ζωής[23]. Οι συσκευές δεν έχουν υψηλή ασφάλεια από την σχεδίασή τους και πρέπει να βρεθούν λύσεις για την προστασία τους από φυσικές επιθέσεις και καταστροφές. Για να γίνει αυτό, χρησιμοποιούνται διάφορες τεχνικές και αλγόριθμοι για την ασφαλή μεταφορά και επεξεργασία των δεδομένων.

5.1 Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση είναι η διαδικασία του μετασχηματισμού των δεδομένων σε μορφή που δεν μπορεί να διαβαστεί χωρίς την χρήση του σωστού κλειδιού σε συνδυασμό με τον αλγόριθμο κρυπτογράφησης. Χρησιμοποιείται κυρίως για την εξασφάλιση της εμπιστευτικότητας των δεδομένων.

Υπάρχουν δύο βασικά είδη κρυπτογράφησης: η συμμετρική και η ασύμμετρη.

Στην συμμετρική κρυπτογράφηση χρησιμοποιείται κοινό κλειδί (ιδιωτικό κλειδί) για την κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων και θεωρείται ο γρηγορότερος από τους δυο τύπους. Στην ασύμμετρη κρυπτογράφηση χρησιμοποιείται διαφορετικό κλειδί (δημόσιο κλειδί) για την κρυπτογράφηση και διαφορετικό (ιδιωτικό κλειδί) για την αποκρυπτογράφηση.

Το βασικό χαρακτηριστικό των IoT είναι η χαμηλή τιμή τους, η ενεργειακή απόδοση τους, λόγω της χαμηλής επεξεργαστικής ισχύος τους, και η διαλειτουργικότητά τους. Για τον λόγο αυτό, δεν μπορούν να χρησιμοποιηθούν οι παραδοσιακοί αλγόριθμοι κρυπτογράφησης (DES, RSA) επειδή απαιτούν μεγάλη υπολογιστική ισχύ άρα και υψηλή χωρητικότητα μπαταρίας και μεγάλη χωρητικότητα μνήμης. Όπως γίνεται αντιληπτό, με αυτούς τους αλγορίθμους οι IoT συσκευές δεν θα λειτουργούν αποδοτικά και σε κάποιες περιπτώσεις (sensors, RFID tags) μπορεί και καθόλου. Έτσι, πρέπει να χρησιμοποιηθούν αλγόριθμοι χαμηλού κόστους πόρων που μπορούν να λειτουργήσουν αποδοτικά με βάση αυτά τα χαρακτηριστικά των IoT συσκευών.

Για την πραγματοποίηση αυτού του σκοπού έχει δημιουργηθεί ένα συγκεκριμένο είδος κρυπτογράφησης, που ονομάζεται lightweight (ελαφριά). Οι περισσότεροι αλγόριθμοι που σχεδιάζονται με αυτή την προδιαγραφή, χρησιμοποιούν μικρά μεγέθη κλειδιών και block (μέγεθος δεδομένων που επεξεργάζεται ο αλγόριθμος κάθε στιγμή).

Τα βασικά χαρακτηριστικά των lightweight αλγορίθμων κρυπτογράφησης παρουσιάζονται στον παρακάτω Πίνακα 1:

Characteristics		What LWC can offer?
Physical (Cost)	Physical Area(GEs, logic blocks)	Smaller block sizes (64-bit or less) Smaller key size (80-bit or less) Simple round logic based on simple computations Simple key scheduling
	Memory (registers, RAM, ROM)	
	Battery power (energy consumption)	
Performance	Computing Power (latency, throughput)	
Security	Minimum security strength (bits)	Strong Structure (like SPN or FNS)
	Attack models (related key, multi- keys)	
	Side channel attack	

Πίνακας 1. Βασικά χαρακτηριστικά lightweight αλγορίθμων κρυπτογράφησης arxiv.org/pdf/2006.13813

Ένας πολύ γνωστός lightweight αλγόριθμος κρυπτογράφησης είναι ο Elliptic Curves Cryptography (ελλειπτικές καμπύλες) αλγόριθμος, ο οποίος είναι ασύμμετρος και χρησιμοποιεί μικρότερο κλειδί σε σχέση με άλλους διάσημους αλγορίθμους και χρησιμοποιείται συχνά σε IoT συσκευές[24] αλλά και κινητά τηλέφωνα.

Μια οικογένεια lightweight αλγορίθμων κρυπτογράφησης, που ονομάζεται Ascon, έχει μεγάλη απήχηση τα τελευταία χρόνια και είναι ο αλγόριθμος που προτιμάται για την χρήση σε μικρές και αδύναμες συσκευές. Μεγάλο μέρος αυτής της διασημότητας προήλθε μετά από τον Φεβρουάριο του 2023, όπου επιλέχθηκε από τον NIST (National Institute of Standards and Technology, Εθνικό Ινστιτούτο Τυποποίησης και Τεχνολογίας των ΗΠΑ) ως πρότυπο για την ασφαλή χρήση του σε μικρές συσκευές. Συγκεκριμένα, ο αλγόριθμος αυτός λειτουργεί πολύ αποδοτικά σαν εργαλείο για κατακερματισμό (hashing) αλλά και για χρήση σε συστήματα ταυτοποίησης[25].

Κάποιες IoT συσκευές που μπορεί να κάνουν πιο απαιτητική δουλειά, έχουν πιο δυνατό υλικό και άρα δεν είναι αναγκαία η χρήση lightweight αλγορίθμων κρυπτογράφησης. Σε αυτές τις περιπτώσεις, θα χρησιμοποιηθούν οι γνωστοί αλγόριθμοι που είναι αποδοτικοί και προστατεύουν τα δεδομένα με μεγάλη πιθανότητα. Κάποιοι από αυτούς τους αλγόριθμοι είναι οι: AES, BLOWFISH, RSA, DES[31].

Ο κατακερματισμός (hashing) χρησιμοποιείται συχνά για την αποθήκευση κωδικών πρόσβασης, τη δημιουργία ψηφιακών υπογραφών και την επαλήθευση της ακεραιότητας δεδομένων.Ένας από τους πιο χρησιμοποιόμενους αλγόριθμους είναι ο SHA-256 (Secure Hash Algorithm)όπου είναι μέρος της οικογένειας αλγορίθμων SHA 2. Δημοσιεύτηκε το 2001, ήταν μια κοινή προσπάθεια μεταξύ της NSA και της NIST για να εισαγάγουν έναν διάδοχο της οικογένειας SHA 1, η οποία έχανε σιγά σιγά τη δύναμή της ενάντια στις επιθέσεις ωμής βίας. Η σημασία του 256 στο όνομα αντιπροσωπεύει την τελική τιμή σύνοψης κατακερματισμού, δηλαδή ανεξάρτητα από το μέγεθος του απλού κειμένου/καθαρού κειμένου, η τιμή κατακερματισμού θα είναι πάντα 256 bit[32].

5.2 Προηγμένα συστήματα ταυτοποίησης και πιστοποίησης

Η πιστοποίηση και η ταυτοποίηση σε πληροφοριακά συστήματα είναι άκρως απαραίτητες επειδή βεβαιώνουν την ασφαλή διασύνδεση συσκευής και ανθρώπου (εξουσιοδοτημένου χρήστη) ή άλλου τελικού προορισμού των δεδομένων (π.χ. έναν server) και προφυλάσσουν από την μη εξουσιοδοτημένη πρόσβαση των συστημάτων από κακόβουλους παράγοντες.[26]

Όταν ένα σύστημα έχει χαμηλό επίπεδο πιστοποίησης και η ταυτοποίησης υπάρχουν πολλοί τρόποι με τους οποίους ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε αυτό (DoS, DDoS attacks), όπου μετά μπορούν να προκαλέσουν σοβαρές ζημιές στην υποδομή που χρησιμοποιούνται αφού μπορούν να καταργήσουν τις υπηρεσίες της. Στον πίνακα 2[6] παρουσιάζονται κάποια βασικά είδη επιθέσεων που παραβιάζουν τον έλεγχο πρόσβασης στις συσκευές με τέτοιες υποδομές:

Attacks	Description
Masquerade Attack	In this attack, adversary counterfeit identity of the legitimate user to get access to the network.
Man-in-the-middle Attack	In this attack, attackers inquire impertinently communication between two communicators.
DoS Attack	In this attack, attackers flood the network by spreading inconvenient packets and disrupt actual communication to penetrate the network.
Forging Attack	In this attack, an adversary emulates a system or authenticated user to gain access to the network.
Guessing Attack	In this attack, attackers predict and explore the possibilities of getting advantages over the credentials of legal users.
Physical Attack	In this attack, network enemies try to get access to the physical components. In addition, they may penetrate the network or inject malicious scripts into the network, after getting physical access
Routing Attack	In this attack, attackers create an improper route to send or receive packets in a network.

Πίνακας 2. Επιθέσεις στην αυθεντικοποίηση source: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8871112

Για την αποφυγή τέτοιων σεναρίων χρησιμοποιούνται διάφορες αρχιτεκτονικές που αναφέρουν τρόπους που διασφαλίζουν ποιοι χρήστες ή ποια συστήματα μπορούν να επικοινωνήσουν με κάποια συσκευή, περιορίζοντας έτσι πιθανές επιθέσεις.
Επειδή υπάρχει ένας τεράστιος αριθμός IoT συσκευών, νούμερο που όλο και μεγαλώνει με το πέρασμα του χρόνου, που είναι συνδεδεμένες μεταξύ τους και επικοινωνούν η μια με την άλλη σε αληθινό χρόνο, το πρόβλημα του ελέγχου πρόσβασης γίνεται όλο και πιο σημαντικό, και αναλογικά, όλο και πιο δύσκολη η επίλυσή του. Οι ποιο συνηθισμένοι και εύκολοι τρόποι αυθεντικοποίησης στις IoT συσκευές είναι η χρήση σταθερού μυστικού κωδικού, η χρήση token-based πιστοποίησης, δηλαδή η χρήση κωδικού ή άλλου είδους δεδομένων, μιας χρήσης, που ισχύουν για μόνο εκείνη την χρονική στιγμή. Επίσης, χρησιμοποιείται, αν και πιο ακριβός, βιομετρικός έλεγχος (δακτυλικό αποτύπωμα, ίριδα του ματιού, έλεγχος του προσώπου) αλλά και lightweight κρυπτογράφηση, όπως αναφέραμε προηγουμένως[27]. Επίσης, μπορεί να χρησιμοποιηθούν υποδομές νέφους (cloud) σαν μέσο για την ασφαλή σύνδεση IoT συσκευών με τον χρήστη, αλλά και για την ασφαλή μεταφορά των δεδομένων [28].

Ένας αλγόριθμος που χρησιμοποιείται πολύ συχνά για ταυτοποίηση είναι ο ασύμμετρος αλγόριθμος κρυπτογράφησης RSA που χρησιμοποιείται και για την δημιουργία ψηφιακών υπογραφών. Για τις ψηφιακές υπογραφες (digital signatures) χρησιμοποιούνται κρυπτογραφικές τεχνικές για να δημιουργηθεί ένας κωδικό (η υπογραφή) που είναι μοναδικός τόσο για τον υπογράφοντα όσο και για το περιεχόμενο. Αυτό διασφαλίζει όχι μόνο την ταυτότητα του υπογράφοντος, αλλά και επαληθεύει ότι το έγγραφο δεν έχει παραβιαστεί μετά την υπογραφή [33].

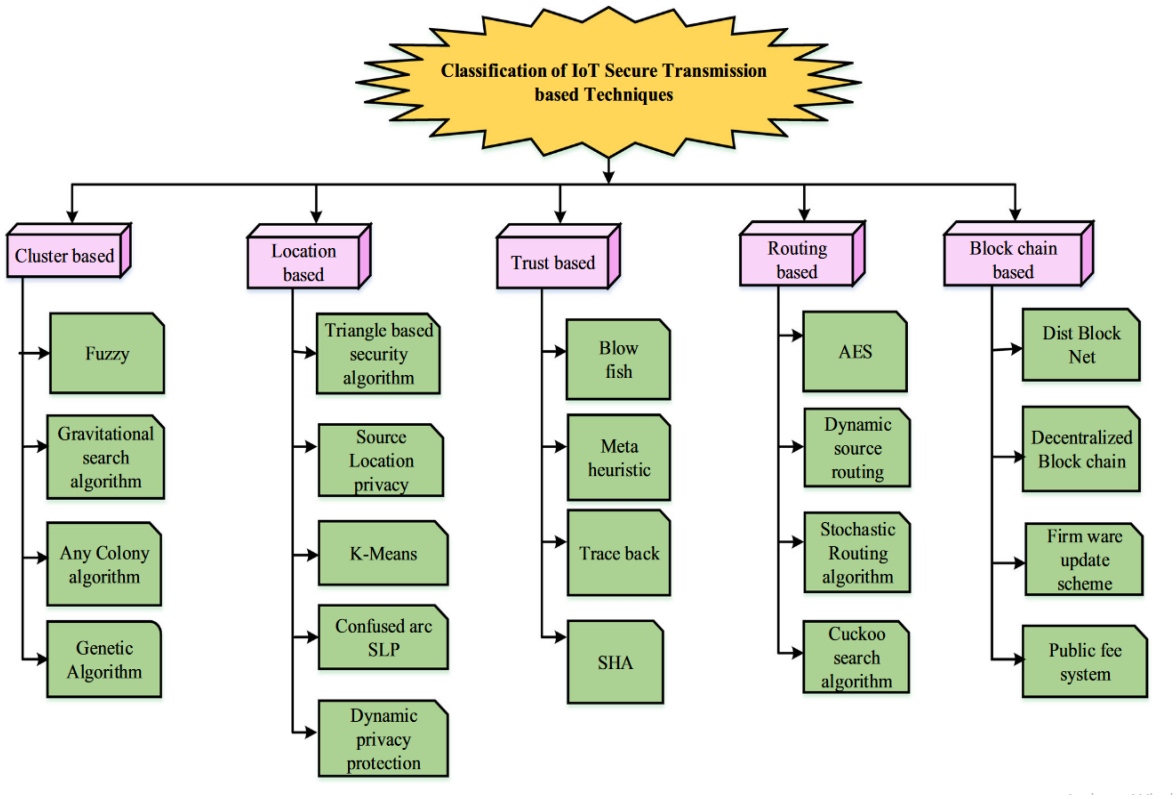
Επιπλέον, ο BLOWFISH αλγόριθμος κρυπτογράφησης, που εμφανίζεται συχνά σε IoT συσκευές, λόγω της εύκολη εγκατάστασής του σε επίπεδο υλικού[34], συναντάται σε συστήματα ταυτοποίησης. Είναι ένας συμμετρικός αλγόριθμος και χρησιμοποιεί μεσαίο μέγεθος μπλοκ για την κρυπτογράφηση, σε σχέση με πιο δυνατούς όπως ο AES και είναι καλύτερος του DES, αφού είναι γρηγορότερος[35].

5.3 Ασφαλής μετάδοση δεδομένων

Με την ασφαλή μετάδοση δεδομένων αναφερόμαστε στον τρόπο που θα επικοινωνήσουν δύο συσκευές, συνήθως μέσω του διαδικτύου, ώστε να ανταλλάξουν πληροφορίες, εξασφαλίζοντας, κυρίως, την ακεραιότητα και εμπιστευτικότητα τους. Για την επίτευξη της ασφαλής μετάδοσης των δεδομένων χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης αλλά και τεχνικές για την διασφάλιση του δικτύου που χρησιμοποιείται για την επικοινωνία.

Στις IoT συσκευές για λόγους απόδοσης αλλά και το χαρακτηριστικό τους ότι μπορούν να είναι συνδεδεμένες με πολλά διαφορετικά δίκτυα κάθε στιγμή, η χρήση lightweight κρυπτογράφησης για την ασφαλή μεταφορά των δεδομένων είναι μονόδρομος. Όμως, με την διασφάλιση της εμπιστευτικότητας των δεδομένων με την κρυπτογράφησή τους, δεν προστατεύονται από άλλα είδη επιθέσεων που ,για παράδειγμα, παραβιάζουν την ακεραιότητα ή την διαθεσιμότητά τους, η οποία είναι πολύ σημαντική στο πλαίσιο των IoT συσκευών. Για την ασφάλεια των δεδομένων χρησιμοποιούνται διάφορες τεχνικές όπου τα προστατεύουν με βάση τον τρόπο που στέλνονται στον τελικό προορισμό. Παραδείγματος χάριν, τα δεδομένα μπορεί να στέλνονται με βάση την τοποθεσία της κάθε συσκευής, δηλαδή ανάλογα με την απόσταση από το κεντρικό σημείο συσσώρευσης των δεδομένων (κάποιον server) ή με βάση κάποια ιεραρχική προσέγγιση, δηλαδή όλα τα δεδομένα μαζεύονται σε μια συγκεκριμένη συσκευή που έχει ασφαλιστεί, με χρήση αλγορίθμων κρυπτογράφησης, και από εκεί στέλνονται στον τελικό τους προορισμό. Επίσης, με τις blockchain τεχνολογίες να μεγαλώνουν σε διασημότητα, έχουν γίνει άλλος ένας τρόπος για την προστασία των δεδομένων όταν αυτά συλλέγονται και μεταφέρονται σε μεγάλο αριθμό διαφορετικών συσκευών όπως γίνεται στις IoT υποδομές[29].

Στον πίνακα 3 παρουσιάζεται ένα σχήμα με τεχνικές διασφάλισης των δεδομένων με βάση διάφορες προσεγγίσεις μετάδοσης δεδομένων:



Πίνακας 3. Τεχνικές διασφάλισης δεδομένων με βάση προσεγγίσεων μετάδοσης δεδομένων

www.researchgate.net/publication/340994537_A_Survey_on_Secure_Transmission_in_Internet_of_Things_Taxonomy_Recent_Techniques_Research_Requirements_and_Challenges

Ο AES, ο οποίος είναι συμμετρικός αλγόριθμος, είναι από τους πιο δυνατούς αλγόριθμους κρυπτογράφησης επειδή χρησιμοποιεί μεγάλο κλειδί για την κρυπτογράφηση και χρησιμοποιείται συνήθως για την διασφάλιση της εμπιστευτικότητας των δεδομένων. Για αυτό, χρησιμοποιείται όταν πρέπει να μεταφερθούν ευαίσθητα δεδομένα μέσα από ένα πιθανώς μη ασφαλές κανάλι επικοινωνίας.

Μπορεί να συνδυαστεί και με τον RSA αλγόριθμο με μια ψηφιακή υπογραφή, που αναφέρθηκαν παραπάνω, για να διασφαλιστεί ταυτόχρονα και η ακεραιότητα των δεδομένων που στέλνονται.

6. Προβλήματα και Λύσεις απορρήτου στο Διαδίκτυο των Πραγμάτων

Το IoT ανοίγει νέους ορίζοντες για φορητές και οικιακές συσκευές, αλλά εισάγει και νέες παγίδες σχετικά με τον διαμοιρασμό των πληροφοριών στο Διαδίκτυο. Τα δεδομένα περιέχουν μεγάλο όγκο προσωπικών πληροφοριών και δυστυχώς δίνεται προτεραιότητα στην γρήγορη διακίνηση των IoT και πολύ συχνά η διατήρηση της ασφάλειας αυτών παραμελείται. Τα προβλήματα που έχουν καταγραφεί ποικίλλουν όμως προκύπτουν ταυτόχρονα και ευρηματικές λύσεις. Το σημαντικότερο όμως, είναι οι εξέλιξη των λύσεων να είναι ταχύτερη από την εξέλιξη των ζητημάτων ασφαλείας.

Ένα τυπικό σύστημα IoT αποτελείται από τους παρακάτω 3 παράγοντες: Έξυπνες συσκευές, εφαρμογές και λογισμικό IoT, και User Interface (UI). Ο κύριος διαχωρισμός των προκλήσεων αφορά δύο μεγάλες κατηγορίες: τη πολιτική της συλλογής των δεδομένων και την ανωνυμοποίηση τους. Ανάλογα με τις τεχνολογίες των smart objects, υπάρχουν οι αντίστοιχες ανησυχίες για την ιδιωτικότητας τους.

6.1 Προβλήματα απορρήτου στα έξυπνα Σπίτια (Smart Homes)

Τα έξυπνα σπίτια αναφέρονται σε κατοικίες με εγκαταστάσεις συσκευών ή υπηρεσιών που μπορούν να ελέγχονται αυτόματα και εξ αποστάσεως απο οπουδήποτε με σύνδεση στο διαδίκτυο, μέσω κινητής συσκευής ή άλλης αντίστοιχης συσκευής. Οι υπηρεσίες που προσφέρονται δίνουν τη δυνατότητα στο χρήστη/ στους χρήστες να ελέχγουν λειτουργίες όπως την πρόσβαση ασφαλείας στο σπίτι, τη θερμοκρασία, τον φωτισμό, το πότισμα του κήπου, τη λειτουργία των οικιακών ηλεκτρικών συσκευών, παρακολούθηση βρέφους / κατοικιδίων μέσω κάμερας κλπ.

Τα προβλήματα που αναδύονται από τη χρήση των παραπάνω υπηρεσιών προσβάλλουν την ασφάλεια των χρηστών σε βασικό επίπεδο, θέτοντας τις αρχές της ακεραιότητας, αυθεντικοποίησης και πρόσβασης σε κίνδυνο. Η ανεπιθύμητη αποκάλυψη ευαίσθητων πληροφοριών, η παραποίηση πληροφοριών ελέγχου και η μη εξουσιοδοτημένη πρόσβαση στα συστήματα ελέγχου είναι λόγοι για τους οποίους οι χρήστες πρέπει να είναι ευαισθητοποιημένοι ως προς την επιλογή κατάλληλων IoT που συμμορφώνονται με πρότυπα και κανόνες. Για παράδειγμα, η αποκάλυψη πληροφοριών κατανάλωσης ενέργειας μπορεί να ενημερώσει πιθανούς παραβάτες για τις ώρες απουσίας των κατοίκων. Επίσης, η παραβίαση ενός συστήματος ασφαλείας μπορεί να επιτρέψει την ανεξέλεγκτη πρόσβαση στο σπίτι και να υποβάλλει τους χρήστες σε ψηφιακό ή ακόμα σωματικό κίνδυνο.

6.2 Προβλήματα απορρήτου στις έξυπνες Πόλεις (Smart Cities)

Οι έξυπνες πόλεις (smart cities) είναι κατοικήσιμες περιοχές όπου χρησιμοποιούν τη συλλογή δεδομένων με σκοπό τη βελτίωση της ποιότητας ζωής των κατοίκων, λύνοντας πρακτικά ζητήματα από την εύρεση πάρκινγκ ως τα συστήματα παρακολούθησης του κλίματος και της αποχέτευσης. Αυτά τα δεδομένα χρησιμοποιούνται για την προσαρμογή των λειτουργιών της πόλης, για την αύξηση της βιωσιμότητας και τη βελτίωση της αποδοτικότητας της κοινωνίας. Προάγουν επίσης την καινοτομία και διευκολύνουν την καλύτερη διαχείριση των πόρων, δημιουργώντας ένα πιο ευχάριστο και λειτουργικό αστικό περιβάλλον.

Το πολυτιμότερο συστατικό μιας έξυπνης πόλης είναι τα δεδομένα. Καθώς οι πόλεις γίνονται πιο ψηφιακές, οι ανησυχίες για την ιδιωτικότητα των δεδομένων και την κυβερνοασφάλεια γίνονται πρωταρχικές. Η προστασία των τεράστιων ποσοτήτων δεδομένων που συλλέγονται από έξυπνες συσκευές αποτελεί σημαντική πρόκληση που απαιτεί ισχυρά πρωτόκολλα ασφαλείας και συνεχή παρακολούθηση. Ενα πρόβλημα απορρήτου είναι η προστασία των δεδομένων απο

επιτιθέμενους, καθώς η πρόσβαση των δεδομένων από μη εξουσιοδοτημένους παράγοντες μπορεί να οδηγήσει σε καταστροφικά αποτελέσματα. Επίσης, η χρηματοδότηση της κατασκευής μιας έξυπνης πόλης υλοποιείται είτε μέσω δημόσιων είτε μέσω ιδιωτικών καναλιών, και οι προθέσεις του αρμόδιου φορέα μπορεί να μην είναι ξεκάθαρες και αυστηρά καθορισμένες, με αποτέλεσμα τα δεδομένα που συλλέγονται να καταλήγουν σε τρίτους για την εξυπηρέτηση τρίτων σκοπών. Το πεδίο των θεμάτων διακυβέρνησης και πολιτικής απαιτεί αλλαγές στους τοπικούς νόμους, κανονισμούς και πολιτικές, κάτι που μπορεί να είναι χρονοβόρο και πολιτικά ευαίσθητο. Επιπλέον, τα δεδομένα μπορεί να χρησιμοποιηθούν για την παρακολούθηση των πολιτών και για άλλες μη δημοκρατικές πρακτικές καταπατώντας κάθε δικάιωμα του πολίτη.

6.3 Προβλήματα απορρήτου στις έξυπνες Υγειονομικές Συσκευές (Smart Healthcare Devices)

Τα συστήματα υγειονομικής περίθαλψης που βασίζονται στο Διαδίκτυο των πραγμάτων ενσωματώνουν προηγμένες τεχνολογίες, όπως συσκευές και αισθητήρες, για να επιτρέπουν την άμεση συλλογή και ανάλυση δεδομένων. Οι τεχνολογίες αυτές διευκολύνουν τη λήψη αποφάσεων σε πραγματικό χρόνο για τη παρακολούθηση της υγείας των ασθενών, τη βελτίωση της ποιότητας της περίθαλψης και τη μείωση του συνολικού κόστους της υγειονομικής περίθαλψης. Χάρη στις συσκευές και τους αισθητήρες IoT, είναι δυνατή η εξ αποστάσεως παρακολούθηση και διαχείριση της κατάστασης των ασθενών, επιτρέποντας την ταχύτερη και αποτελεσματικότερη ανταπόκριση στις ανάγκες τους.

Τα δεδομένα που συλλέγονται από τις έξυπνες συσκευές υγειονομικής περίθαλψης είναι εξαιρετικά ευαίσθητα και κρίσιμα. Καθώς τα δεδομένα υγείας συλλέγονται και διαβιβάζονται από συσκευές και αισθητήρες IoT, υπάρχει κίνδυνος να παραβιαστεί το απόρρητο των πληροφοριών των ασθενών. Η πρόσβαση και η επεξεργασία δεδομένων από μη εξουσιοδοτημένα άτομα οδηγεί σε κατάχρηση των πληροφοριών με σοβαρές συνέπειες για την ιδιωτικότητα των ασθενών. Επιπλέον, η αποθήκευση και η επεξεργασία των δεδομένων καθιστά τα δεδομένα εκτεθειμένα σε επιθέσεις στον κυβερνοχώρο.

6.4 Λύσεις προκλήσεων στα έξυπνα σπίτια, έξυπνες πόλεις και έξυπνη υγεία

Για να αντιμετωπιστούν όλες οι παραπάνω προκλήσεις για την προστασία της ιδιωτικότητας και την ασφάλεια στα έξυπνα σπίτια, τις έξυπνες πόλεις και την έξυπνη υγεία, είναι αναγκαίο να σχεδιαστούν και να χρησιμοποιηθούν καινοτόμες λύσεις. Η υιοθέτηση προτύπων ασφαλείας, όπως το ISO , τα οποία προβλέπουν διαδικασίες διαχείρισης της ασφάλειας των δεδομένων , μπορεί να προστατεύσει τις πληροφορίες από μη εξουσιοδοτημένη πρόσβαση. Η συμμόρφωση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) εγγυάται ότι η συλλογή και η επεξεργασία των δεδομένων διενεργείται με σεβασμό στην ιδιωτική ζωή των χρηστών. Οι τεχνικές μετριασμού των κινδύνων και η χρήση κρυπτογράφησης για την αποθήκευση και τη διαβίβαση δεδομένων αυξάνουν την ασφάλεια, διασφαλίζοντας ότι τα δεδομένα διατηρούνται

προστατευμένα σε κάθε στάδιο. Επιπροσθέτως, οι μέθοδοι ταυτοποίησης και ελέγχου ταυτότητας διασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση σε ευαίσθητες πληροφορίες. Συνδυάζοντας όλα τα παραπάνω η ιδιωτικότητα στα έξυπνα σπίτια, τις έξυπνες πόλεις και την έξυπνη υγεία είναι εφικτή και σίγουρη.

7. Συμπεράσματα και Προοπτικές

Όσο η χρήση IoT συσκευών αυξάνεται συνεχώς, απαιτείται όλο και περισσότερη προσοχή στα δεδομένα που παράγουν και επεξεργάζονται αυτές οι συσκευές. Συλλέγοντας όλες τις παραμέτρους από τις οποίες η κατασκευή, ο προγραμματισμός, η διακίνηση και πιθανή απόσυρση των IoT συσκευών εξαρτάται από τις κανονιστικές και ρυθμιστικές αρχές, τα πρότυπα, καθώς και τις ασφαλείς μεθόδους ανάπτυξης των συστημάτων, χτίζονται τα κατάλληλα θεμέλια για την δημιουργία ολοκληρωμένου και καθολικά εφαρμόσιμου οικοσυστήματος για το IoT.

Πρότυπα, όπως το ISO, που προτυποποιούν μεθόδους προστασίας υπολογιστικών συστημάτων, αρα και συσκευές IoT, ορίζουν γενικές κατευθύνσεις στους οργανισμούς για την σωστή και επαρκή προστασία των δεδομένων τους. Συνήθως, προτείνουν διάφορους αλγορίθμους και τεχνολογίες που έχουν δοκιμαστεί κάτω από αληθινές καταστάσεις και έχουν αποδειχτεί ότι προσφέρουν αρκετή ασφάλεια. Επομένως, για τη διασφάλιση των δεδομένων από διάφορες μορφές επιθέσεων, είναι επιτακτική η χρήση αλγορίθμων κρυπτογράφησης τόσο στην αποθήκευση όσο και στη μεταφορά των δεδομένων, καθώς και η εφαρμογή μηχανισμών ταυτοποίησης.

Η προθυμοποίηση και συνεισφορά των επιχειρήσεων που δραστηριοποιούνται στον τομέα των IoT για την εφαρμογή μιας ολιστικής προσέγγισης της διασφάλισης της ιδιωτικότητας, θα αποδειχθεί μελλοντικά χρήσιμη και θα αποτελέσουν παράδειγμα για τις ανερχόμενες επιχειρήσεις. Ωστόσο, όλα τα παραπάνω μέτρα πρέπει τελικά να επιβληθούν στους οργανισμούς και να υπάρχει συστηματική παρακολούθηση από τις αρμόδιες αρχές, ώστε να διασφαλιστεί η συμμόρφωση και πρωτίστως η προστασία της ιδιωτικότητας των χρηστών.

Κρίνεται λοιπόν απαραίτητο, στην εποχή που η πληροφορία είναι πολύτιμη, να δοθεί η πρέπουσα σημασία στην προστασία των προσωπικών δεδομένων των χρηστών. Οι επιπόλαιες και γρήγορες λύσεις στην ανάπτυξη των IoT, είναι ένα πρόβλημα που δεν συνάδει με την λαμπρή εποχή της τεχνολογίας που διανύουμε, και είναι σημαντικό να αναδεικνύεται το ζήτημα, για να ευαισθητοποιηθούν οργανισμοί επιχειρήσεις και καταναλωτές, με απώτερο σκοπό την εξέλιξη και τη καινοτομία.

Οι προτάσεις για περαιτέρω έρευνα που προκύπτουν από τα παραπάνω συμπεράσματα αφορούν την βελτίωση της αρχιτεκτονικής, της σχεδίασης των IoT και των δικτύων τους. Φέτος αναμένεται πιο αυστηρή ρύθμιση και κατευθυντήριες γραμμές, ειδικά εντός της Ευρωπαϊκής

Ένωσης, για να εξασφαλιστεί ότι τα δεδομένα που συλλέγονται από τις συσκευές IoT διαχειρίζονται με ασφάλεια και ηθική. Η χρήση πιο προηγμένων πρωτοκόλλων κρυπτογράφησης και πολυπαραγοντικής αυθεντικοποίησης για την προστασία από μη εξουσιοδοτημένη πρόσβαση και διαρροές δεδομένων, είναι επίσης ζήτημα των τεχνικών κρυπτογράφησης και ανάπτυξης ισχυρών μηχανισμών αυθεντικοποίησης που επιδέχεται πολλή έρευνα. Όσον αφορά την πολυπαραγοντική αυθεντικοποίηση IoT με χρήση βιομετρικών, η τεχνολογική διάσταση αντιμετωπίζει νέες απειλές, οι οποίες είναι αδιαμφισβήτητης σημαντικότητας να ληφθούν υπόψιν.

Επομένως, πέρα από τα στοιχεία που έχουμε καλύψει σε αυτήν τη βιβλιογραφική εργασία, οι προκλήσεις ασφαλείας στα IoT και γενικότερα, μεταβάλλονται διαρκώς. Το βασικότερο, λοιπόν, που πρέπει να εξεταστεί είναι το πώς θα καταφέρουμε την προσαρμογή των IoT στις εξελίξεις, και προτίστως να προβλέπονται οι αναδυόμενοι κίνδυνοι.

Βιβλιογραφία

[1] https://gdprinfo.eu/el/el-article-4

[2] https://gdpr-info.eu/art-5-gdpr/ άρθρο 5 (1α)

[3] https://gdpr-info.eu/art-5-gdpr/ άρθρο 5 (1c)

[4] https://gdpr-info.eu/art-17-gdpr/

[5] https://gdpr-info.eu/art-15-gdpr/

[6] https://gdpr-info.eu/art-16-gdpr/

[7] https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/how-should-requests-individuals-be-dealt_en

[8] https://gdpr-info.eu/art-5-gdpr/ άρθρο 5 (2)

[9] https://gdpr-info.eu/art-24-gdpr/ άρθρο 24 (1,2)

[10] https://gdpr-info.eu/art-28-gdpr/ άρθρο 24 (3)

[11] https://gdpr-info.eu/art-32-gdpr/

[12] https://gdpr-info.eu/art-4-gdpr/

[13] https://gdpr-info.eu/art-5-gdpr/ άρθρο 5(1c)

[14] https://gdpr-info.eu/art-5-gdpr/ άρθρο 5(1b)

[15] https://gdpr-info.eu/art-32-gdpr/ άρθρο 32(1b)

[16] https://gdpr-info.eu/art-25-gdpr/ άρθρο 25(1)

[17] https://gdpr-info.eu/art-25-gdpr/ άρθρο 25(2)

[18] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ), 119 OJ L § (2016), άρθρο 129. http://data.europa.eu/eli/reg/2016/679/oj/ell.

[19] "Charter of Fundamental Rights of the European Union.Pdf.", άρθρο 7, 8, 12 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN.

[20] : ETSI EN 303 645 V2.1.1 (2020-06) https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

[21] : "Guidelines for Privacy and Security in IoT", Simone Seminara, Francesco Capparelli Istituto Italiano per la Privacy e la Valorizzazione dei Dati Rome, Italy. https://ceur-ws.org/Vol-2739/paper_3.pdf

[22]: Altulaihan, Esra, Mohammed Amin Almaiah, and Ahmed Aljughaiman. “Cybersecurity Threats, Countermeasures and Mitigation Techniques on the IoT: Future Research Directions.” *Electronics* 11, no. 20 (January 2022): 3330. https://doi.org/10.3390/electronics11203330.

[23]: https://arxiv.org/pdf/1901.07309

[24]: Muhammad Rana, Quazi Mamun, Rafiqul Islam, Lightweight cryptography in IoT networks: A survey, Future Generation Computer Systems, Volume 129, 2022, Pages 77-89, ISSN 0167-739X, https://doi.org/10.1016/j.future.2021.11.011.

[25]:https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices

[26]: Wael Alnahari, Dr. Mohammad Tabrez Quasim. Authentication of IoT Device and IoT Server Using Security Key, 16 February 2021, PREPRINT (Version 2) available at Research Square [https://doi.org/10.21203/rs.3.rs-175858/v2]

[27]: T. Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," in IEEE Access, vol. 7, pp. 151054-151089, 2019, doi: 10.1109/ACCESS.2019.2947723. keywords: {Authentication;Internet of Things;Protocols;Sensor phenomena and characterization;Logic gates;Authentication;authentication protocols;Internet of Things;network attacks;security;wireless sensor network},

[28]: Mohammad, A.; Al-Refai, H.; Alawneh, A.A. User Authentication and Authorization Framework in IoT Protocols. Computers 2022, 11, 147. https://doi.org/10.3390/computers11100147

[29]:Mahapatra, Surya & Singh, Binod & Kumar, Vinay. (2020). A Survey on Secure Transmission in Internet of Things: Taxonomy, Recent Techniques, Research Requirements, and Challenges. Arabian Journal for Science and Engineering. 45. 10.1007/s13369-020-04461-2.

[31]: https://d1wqtxts1xzle7.cloudfront.net/101475070/d62956dba6b71b363e588a2aa4bbb117fcaa-libre.pdf?1682422922=&response-content-disposition=inline%3B+filename%3DA_Survey_on_Cryptography_Algorithms.pdf&Expires=1719501931&Signature=K~yn8N3qFv7Zc5J8CRDzkQKpmpqHHQiDifT6c5JiEltZco9mnbpAXVfOOD1VSaxBVha~9k4byBKKtDSU8SO4a7uDETBTOQLI9NQWqbZQjnjuPhcZaNUyPQozr83WLxo68cxiav9iARsQOtE1ezFr-hZytIePqAijYlndzAcuw8Czjv-HI6XoO3Qpa8UuXyQVWU1JSEaui1cO8NSNtSAfcdihn89KY-~89PlhzFWCHRXS4k2E0PvRjtgjKYKXesaSD0DQ4WU2KLpQbqXWf5JR4ABHJGfPimL70Boz9CgiM2WU0xX0ZRjj9cH-zN8WeUj~XXsgNGAeUJZPfO1Jrjlbgg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

[32]: https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm#what_is_the_sha256_algorithm

[33]: https://www.dock.io/post/digital-signatures

[34]: A. Alabaichi, F. Ahmad and R. Mahmod, "Security analysis of blowfish algorithm," 2013 Second International Conference on Informatics & Applications (ICIA), Lodz, Poland, 2013, pp. 12-18, doi:

10.1109/ICoIA.2013.6650222. keywords: {Barium;Algorithm design and analysis;Correlation coefficient;Ciphers;Encryption;algorithm;avalanche effect;Correlation coefficient},

[35]: https://www.schneier.com/academic/blowfish/

https://peerj.com/preprints/26474.pdf

https://arxiv.org/pdf/1901.07309

Fursan Thabit, Ozgu Can, Asia Othman Aljahdali, Ghaleb H. Al-Gaphari, Hoda A. Alkhzaimi, Cryptography Algorithms for Enhancing IoT Security, Internet of Things, Volume 22, 2023, 100759, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100759.