Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Τηλεπικοινωνίων

Τμήμα Ψηφιακών Συστημάτων

Π.Μ.Σ Κυβερνοασφάλεια και Τεχνολογίες Τεχνητής Νοημοσύνης

Μεταπτυχιακή Διπλωματική Εργασία

Ασφάλεια και Προστασία της Ιδιωτικότητας σε Έξυπνα Σπίτια (Smart Homes)

Δονάτος Ντόλος mte24023

Επιβλέπων Καθηγητής: Στέφανος Γκρίτζαλης

Πειραιάς, Φεβρουάριος 2026

Περίληψη

Η παρούσα εργασία εξετάζει την ασφάλεια και την προστασία της ιδιωτικότητας στα έξυπνα σπίτια, ένα τεχνολογικό οικοσύστημα που εξελίσσεται ταχύτατα και ενσωματώνει ποικίλες συσκευές και υπηρεσίες. Στόχος είναι η διερεύνηση των τεχνικών, οργανωτικών και κοινωνικών παραγόντων που επηρεάζουν την ασφάλεια των smart homes, η αποτύπωση των ευπαθειών που εντοπίζονται σε επίπεδο συσκευών και δικτύων, καθώς και η κατανόηση των αντιλήψεων, ανησυχιών και προσδοκιών των χρηστών αναφορικά με την ιδιωτικότητά τους. Η μελέτη ακολουθεί βιβλιογραφική προσέγγιση, αξιοποιώντας δημοσιευμένες έρευνες, ποσοτικές και ποιοτικές μελέτες, τεχνικές αναλύσεις και case studies από το πεδίο της κυβερνοασφάλειας και της ανθρώπινης-τεχνολογικής αλληλεπίδρασης. Η ανασκόπηση οργανώθηκε θεματικά: αδυναμίες συσκευών και πρωτοκόλλων επικοινωνίας, κατηγορίες επιθέσεων, προσεγγίσεις άμυνας (IDS/IPS, κρυπτογραφία, AI/ML), καθώς και ερευνητικά δεδομένα για τις συμπεριφορές και στάσεις των χρηστών. Τα ευρήματα καταδεικνύουν ότι τα έξυπνα σπίτια παρουσιάζουν σημαντικές τεχνικές ευπάθειες που σχετίζονται με το υλικό, το λογισμικό και τα πρωτόκολλα επικοινωνίας. Παράλληλα, αναδεικνύεται ότι οι χρήστες συχνά δεν διαθέτουν πλήρη επίγνωση των κινδύνων, με αποτέλεσμα να εμφανίζονται φαινόμενα security fatigue και risky behavior. Η ανάλυση των μηχανισμών άμυνας δείχνει ότι ενεργειακοί και υπολογιστικοί περιορισμοί επηρεάζουν την αποτελεσματικότητα των λύσεων ασφάλειας. Επιπλέον, οι μελέτες χρήστη επιβεβαιώνουν υψηλά επίπεδα ανησυχίας για παρακολούθηση, διαρροές δεδομένων και απώλεια ελέγχου. Η ασφάλεια στα smart homes απαιτεί μια ολιστική προσέγγιση που συνδυάζει ασφαλή σχεδιασμό, αξιόπιστα πρωτόκολλα, προηγμένους μηχανισμούς ανίχνευσης απειλών και ενδυνάμωση των χρηστών μέσω διαφανούς και κατανοητής διαχείρισης δεδομένων. Η ενσωμάτωση αρχών secure-by-design και privacy-by-design αποτελεί κρίσιμη προϋπόθεση για την ενίσχυση εμπιστοσύνης και τη βιώσιμη χρήση των έξυπνων οικιακών τεχνολογιών.

Λέξεις Κλειδιά: Ασφάλεια IoT, Έξυπνα σπίτια, Ιδιωτικότητα χρηστών, Κυβερνοαπειλές

Abstract

This study examines security and privacy in smart homes, a rapidly evolving technological ecosystem that integrates a variety of devices and services. The aim is to investigate the technical, organizational, and social factors that affect the security of smart homes, identify vulnerabilities at the device and network level, and understand users' perceptions, concerns, and expectations regarding their privacy. The study takes a bibliographic approach, drawing on published research, quantitative and qualitative studies, technical analyses, and case studies from the fields of cybersecurity and human-technology interaction. The review was organized thematically: weaknesses of devices and communication protocols, categories of attacks, defense approaches (IDS/IPS, cryptography, AI/ML), as well as research data on user behaviors and attitudes. The findings show that smart homes have significant technical vulnerabilities related to hardware, software, and communication protocols. At the same time, it is evident that users are often not fully aware of the risks, resulting in security fatigue and risky behavior. Analysis of defense mechanisms shows that energy and computational constraints affect the effectiveness of security solutions. In addition, user studies confirm high levels of concern about surveillance, data leaks, and loss of control. Security in smart homes requires a holistic approach that combines secure design, reliable protocols, advanced threat detection mechanisms, and user empowerment through transparent and understandable data management. The integration of secure-by-design and privacy-by-design principles is a critical prerequisite for building trust and ensuring the sustainable use of smart home technologies.

Keywords: IoT security, Smart homes, User privacy, Cyber threats

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Περιεχόμενα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

Περιεχόμενα Εικόνων

1. Εισαγωγή

Η ταχεία ανάπτυξη του οικοσυστήματος του Internet of Things (IoT) και η διάχυσή του στο οικιακό περιβάλλον έχουν μετασχηματίσει την έννοια της κατοικίας, εισάγοντας λειτουργίες αυτοματισμού, άνεσης και ενεργειακής αποδοτικότητας που πριν από λίγα χρόνια θεωρούνταν καινοτόμες. Τα έξυπνα σπίτια αποτελούν πλέον ένα πολυσύνθετο πλέγμα διασυνδεδεμένων συσκευών –από αισθητήρες και θερμοστάτες μέχρι κάμερες, έξυπνες κλειδαριές και ολοκληρωμένα συστήματα φωνητικών βοηθών– το οποίο συνδυάζει τεχνολογίες ασύρματης επικοινωνίας, cloud-based υπηρεσίες και εξελιγμένα μοντέλα αυτοματισμού. Η μετάβαση αυτή συνοδεύεται από αδιαμφισβήτητα πλεονεκτήματα, όπως η βελτίωση της ποιότητας ζωής, η δυνατότητα απομακρυσμένου ελέγχου και η αυξημένη ευκολία χρήσης. Παράλληλα, όμως, δημιουργεί ένα νέο τοπίο κινδύνων, όπου η ασφάλεια και η ιδιωτικότητα των χρηστών αποτελούν κρίσιμα ζητήματα με τεχνολογικές, κοινωνικές και ηθικές διαστάσεις.

Σε αυτό το πλαίσιο, πλήθος ερευνών έχει αναδείξει τις διαρθρωτικές αδυναμίες των IoT συσκευών, καθώς και τις πολλαπλές μορφές κυβερνοεπιθέσεων που είναι εφικτές λόγω της ετερογένειας και των περιορισμένων πόρων των συστημάτων αυτών. Ήδη από τις πρώτες μελέτες, ερευνητές δείχνουν ότι οι συσκευές πρώτης γραμμής –όπως αισθητήρες, έξυπνες κάμερες και smart locks– ενσωματώνουν είτε ανεπαρκείς μηχανισμούς αυθεντικοποίησης είτε προβληματικές υλοποιήσεις firmware, επιτρέποντας επιθέσεις χαμηλής έως υψηλής πολυπλοκότητας (π.χ. Alharbi & Aspinall, 2018· Bhardwaj et al., 2023). Παρόμοιες αδυναμίες εντοπίζονται και στα πρωτόκολλα επικοινωνίας, όπου ακόμη και ώριμες τεχνολογίες, όπως τα Wi-Fi και Zigbee, παρουσιάζουν προβλήματα στο key management, στην αυθεντικοποίηση και στην προστασία της ακεραιότητας των πακέτων, με αποτέλεσμα να διευκολύνονται επιθέσεις spoofing, replay και man-in-the-middle (Naidu & Kumar, 2019· Shahidi, 2019· Babun et al., 2020).

Η βιβλιογραφία καταδεικνύει ότι αυτές οι τεχνικές αδυναμίες έχουν άμεσες επιπτώσεις για την ασφάλεια και την ιδιωτικότητα των χρηστών. Πραγματικά περιστατικά και πειραματικές επιθέσεις δείχνουν ότι οι εισβολείς μπορούν να αποκτήσουν πρόσβαση σε οικιακές κάμερες, να τροποποιήσουν αυτοματισμούς, να παρακάμψουν συστήματα ασφαλείας ή να εξάγουν λεπτομερή δεδομένα που αποκαλύπτουν τις συνήθειες και την

παρουσία των ενοίκων (Notra et al., 2014· Sivanathan et al., 2017· Xenofontos et al., 2021). Η πραγματικότητα αυτή καθιστά αναγκαία την ανάπτυξη νέων μοντέλων άμυνας, από κρυπτογραφικά πρωτόκολλα και μηχανισμούς αυθεντικοποίησης μέχρι AI-based συστήματα ανίχνευσης ανωμαλιών και υβριδικές αρχιτεκτονικές IDS/IPS σχεδιασμένες για περιβάλλοντα περιορισμένων πόρων (Dhanda et al., 2020· Eskandari et al., 2020· Rafique et al., 2024).

Ωστόσο, το τεχνικό σκέλος της ασφάλειας αποτελεί μόνο μία διάσταση του ζητήματος. Η συμπεριφορά των χρηστών, οι αντιλήψεις τους για την ιδιωτικότητα και η σχέση τους με την τεχνολογία διαδραματίζουν καθοριστικό ρόλο στη συνολική ανθεκτικότητα των έξυπνων σπιτιών. Μελέτες έχουν δείξει ότι οι χρήστες συχνά υποτιμούν τους κινδύνους ή θεωρούν ότι η ασφάλεια αποτελεί ευθύνη του κατασκευαστή, αναπτύσσοντας ad hoc πρακτικές που δεν ανταποκρίνονται στις σύγχρονες απειλές (Jacobsson & Davidsson, 2015· Zeng et al., 2017). Επιπλέον, τα έξυπνα σπίτια ως πολυχρηστικά περιβάλλοντα δημιουργούν σύνθετες κοινωνικές δυναμικές: χρήστες με διαφορετικά επίπεδα τεχνικής εξοικείωσης, ασύμμετρες σχέσεις ελέγχου εντός του νοικοκυριού και σύγκρουση μεταξύ ευχρηστίας και ασφάλειας, ιδιαίτερα όταν οι μηχανισμοί προστασίας μειώνουν τη χρηστικότητα ή απαιτούν πρόσθετες ενέργειες από τον χρήστη (Distler et al., 2020· Kraemer & Flechais, 2018).

Επιπλέον, η εξάπλωση των έξυπνων υπηρεσιών οδηγεί σε νέα μορφή «οικιακής επιτήρησης», τόσο από συσκευές που συλλέγουν συνεχώς δεδομένα όσο και από τη χρήση υπηρεσιών cloud, οι οποίες μεταφέρουν μέρος της ευθύνης ασφαλούς αποθήκευσης εκτός του ελέγχου του χρήστη. Οι ανησυχίες για παρακολούθηση, profiling ή δευτερογενή χρήση δεδομένων εντείνονται, ιδιαίτερα όταν οι χρήστες δεν διαθέτουν διαφανή εργαλεία ελέγχου ή όταν οι συσκευές εγκαθίστανται σε χώρους με επισκέπτες και bystanders (Barbosa et al., 2020· Percy-Campbell et al., 2024).

Οι τεχνολογικές εξελίξεις συνεχίζουν να μεταβάλλουν το τοπίο, με την τεχνητή νοημοσύνη να εισάγει νέες δυνατότητες αλλά και νέους κινδύνους. Από τη μια πλευρά, η AI επιτρέπει βελτιωμένη πρόβλεψη επιθέσεων, δυναμική προσαρμογή πολιτικών ασφαλείας και εξελιγμένα συστήματα authentication από την άλλη, δημιουργεί νέα ζητήματα διαφάνειας, εξάρτησης από δεδομένα και πιθανότητας σφαλμάτων κρίσης (Mothukuri et al., 2021· Wajid & Sans, 2024).

Σε αυτό το σύνθετο οικοσύστημα, οι τεχνικές αδυναμίες, οι ανθρώπινοι παράγοντες και οι εξελισσόμενες απειλές συνθέτουν ένα περιβάλλον όπου η ασφάλεια των έξυπνων σπιτιών δεν μπορεί να αντιμετωπιστεί μονοδιάστατα. Απαιτείται μια ολιστική προσέγγιση που να εξετάζει ταυτόχρονα τις τεχνικές προκλήσεις, τη συμπεριφορά των χρηστών, τις αρχιτεκτονικές λύσεις και τις κοινωνικές συνέπειες.

Στόχος της παρούσας εργασίας είναι η συστηματική διερεύνηση της ασφάλειας και της ιδιωτικότητας στα έξυπνα σπίτια μέσα από μια ολοκληρωμένη βιβλιογραφική ανασκόπηση. Η εργασία συνδυάζει τεχνικές, κοινωνικές και συμπεριφορικές προσεγγίσεις, ώστε να αναδειχθούν οι κύριες απειλές, οι τεχνολογικές λύσεις, οι δυναμικές χρήσης και οι αντιλήψεις των χρηστών που επηρεάζουν την αποτελεσματικότητα των συστημάτων IoT.

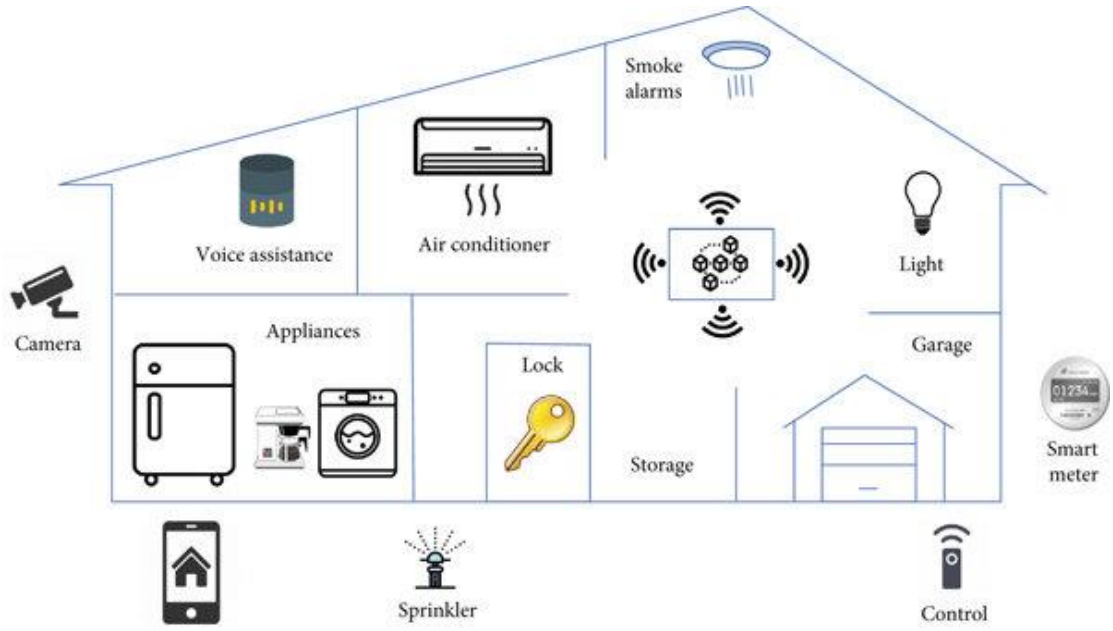
Η εργασία οργανώνεται σε τέσσερα κεφάλαια. Το κεφάλαιο της εισαγωγής, το κεφάλαιο όπου αναλύεται το θεωρητικό πλαίσιο, το κεφάλαιο της βιβλιογραφικής ανασκόπησης όπου πραγματοποιείται η ανάλυση επιθέσεων και τεχνικών αδυναμιών, όπου εξετάζονται συσκευές, πρωτόκολλα και διεισδυτικές τεχνικές, σύγχρονες τεχνολογικές λύσεις, συμπεριλαμβανομένων μηχανισμών αυθεντικοποίησης, κρυπτογραφίας, IDS/IPS και AI-based προσεγγίσεων καθώς και μελέτες ιδιωτικότητας και συμπεριφοράς χρηστών, οι οποίες αναδεικνύουν αντιλήψεις, ανησυχίες και παράγοντες υιοθέτησης ή απόρριψης των έξυπνων συστημάτων. Η εργασία ολοκληρώνεται στο τέταρτο κεφάλαιο με συνθετικά συμπεράσματα, εντοπισμό κοινών θεματικών γραμμών και αναφορά στους περιορισμούς της υφιστάμενης βιβλιογραφίας.

2. Θεωρητικό Πλαίσιο

2.1. Τεχνολογίες έξυπνων σπιτιών

2.1.1. Εισαγωγή στο οικοσύστημα των έξυπνων σπιτιών

Η τεχνολογία των έξυπνων σπιτιών έχει μεταμορφώσει τον τρόπο με τον οποίο αλληλεπιδρούμε με τον οικιακό μας χώρο, προσφέροντας αυτοματοποίηση, βελτιωμένη άνεση και ενεργειακή απόδοση μέσω της ενσωμάτωσης τεχνολογιών Διαδικτύου των Πραγμάτων (IoT). Ένα έξυπνο σπίτι αναφέρεται σε μια κατοικία εξοπλισμένη με σύγχρονη τεχνολογία που μπορεί να προωθήσει την ανεξαρτησία, να επιτρέψει την παρακολούθηση των κατοίκων για ποιοτική διαβίωση και έτσι να βελτιώσει την εμπειρία ζωής (Ezugwu et al., 2025). Στη διάρκεια της τελευταίας δεκαετίας, η παγκόσμια αγορά των έξυπνων σπιτιών έχει παρουσιάσει εκθετική ανάπτυξη, με την αξία της να φτάνει τα 84,5 δισεκατομμύρια δολάρια το 2024 και να αναμένεται να φτάσει τα 116,4 δισεκατομμύρια δολάρια έως το 2029, με σύνθετο ετήσιο ρυθμό ανάπτυξης 6,6% (MarketsandMarkets, 2024).



Εικόνα 1. Παράδειγμα αρχιτεκτονικής και βασικών συσκευών σε ένα έξυπνο οικιακό δίκτυο (smart home network). Πηγή: (Kairaldeen et al., 2021).

Όπως φαίνεται στην Εικόνα 1, ένα τυπικό έξυπνο σπίτι αποτελείται από ένα σύνολο διασυνδεδεμένων συσκευών και υποσυστημάτων, όπως αισθητήρες, κάμερες, έξυπνες οικιακές συσκευές, συστήματα φωτισμού, κλειδαριές και φωνητικούς βοηθούς, τα οποία επικοινωνούν μέσω ασύρματων δικτύων με έναν κεντρικό κόμβο ελέγχου. Η αρχιτεκτονική αυτή επιτρέπει την απομακρυσμένη διαχείριση, την αυτοματοποίηση λειτουργιών και τη συλλογή δεδομένων, δημιουργώντας παράλληλα νέες προκλήσεις ασφάλειας και ιδιωτικότητας.

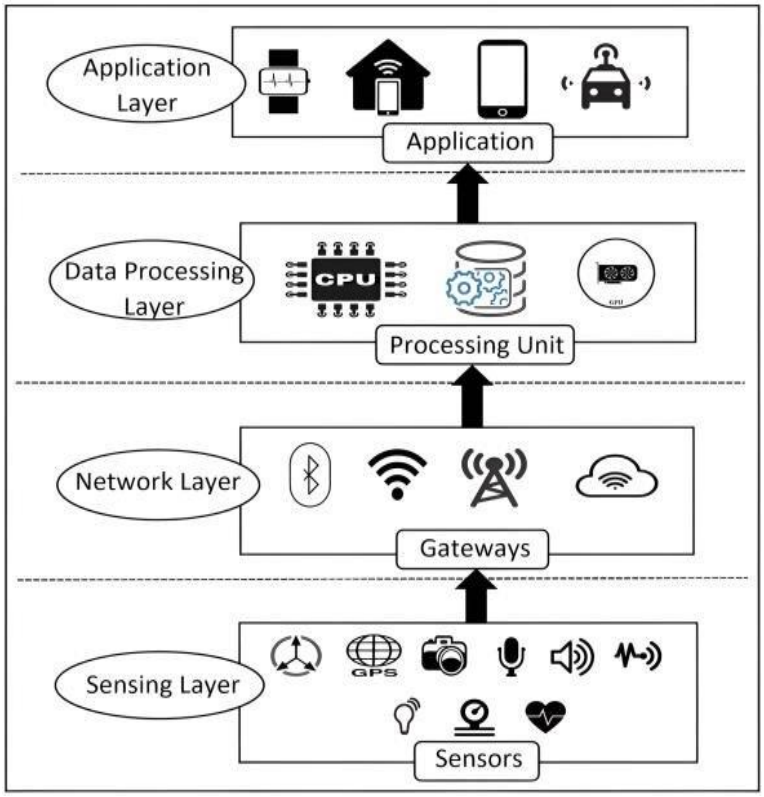
Τα συστήματα έξυπνων σπιτιών επιτρέπουν στους ιδιοκτήτες να ελέγχουν φωτισμό, θέρμανση, εξαερισμό και κλιματισμό (HVAC), συναγερμούς ασφαλείας και άλλες οικιακές συσκευές από απόσταση μέσω των smartphones, tablets ή υπολογιστών τους (MarketsandMarkets, 2024). Τα έξυπνα σπίτια είναι εξοπλισμένα με ενσύρματες και ασύρματες τεχνολογίες επικοινωνίας όπως Wi-Fi, Bluetooth, universal powerline bus (UPB), Insteon, Z-Wave και Zigbee για να προσφέρουν έξυπνες πληροφορίες και λεπτομέρειες στους ιδιοκτήτες παρακολουθώντας συνεχώς διάφορες πτυχές των σπιτιών. Ως μέρος του Διαδικτύου των Πραγμάτων, τα συστήματα και οι συσκευές έξυπνων σπιτιών συχνά λειτουργούν μαζί, μοιράζονται δεδομένα χρήσης καταναλωτών και αυτοματοποιούν ενέργειες με βάση τις προτιμήσεις των ιδιοκτητών.

2.1.2. Αρχιτεκτονική συστημάτων IoT για έξυπνα σπίτια

Η αρχιτεκτονική των συστημάτων IoT αποτελεί τη βασική δομή που επιτρέπει στις διαφορετικές συσκευές στο οικοσύστημα IoT να λειτουργούν αρμονικά μεταξύ τους. Σύμφωνα με τους Burhan et al. (2018), η αρχιτεκτονική IoT μπορεί να διαιρεθεί σε τρία βασικά επίπεδα: το επίπεδο αίσθησης και ενεργοποίησης (sensing and actuating layer), το επίπεδο δικτύου (network layer) και το επίπεδο εφαρμογών (application layer). Στο πρώτο επίπεδο, οι αισθητήρες και οι ενεργοποιητές είναι κυρίως υπεύθυνοι για τη συλλογή δεδομένων ή τη λήψη εντολών από το περιβάλλον. Το επίπεδο δικτύου του συστήματος περιλαμβάνει περιβαλλοντικούς αισθητήρες όπως αυτούς θερμοκρασίας, υγρασίας και CO2, ενώ το επίπεδο εφαρμογών παρέχει διεπαφές χρήστη και υπηρεσίες.

Στην Εικόνα 2 παρουσιάζεται μια τυπική πολυεπίπεδη αρχιτεκτονική IoT, η οποία χρησιμοποιείται ευρέως σε περιβάλλοντα έξυπνων σπιτιών. Η αρχιτεκτονική αυτή διαρθρώνεται σε επίπεδα αίσθησης (sensing layer), δικτύου (network layer), επεξεργασίας δεδομένων (data processing layer) και εφαρμογών (application layer),

επιτρέποντας τη συλλογή δεδομένων από αισθητήρες, τη μετάδοσή τους μέσω πυλών επικοινωνίας, την επεξεργασία τους σε υπολογιστικές μονάδες και την τελική παροχή υπηρεσιών προς τον χρήστη.

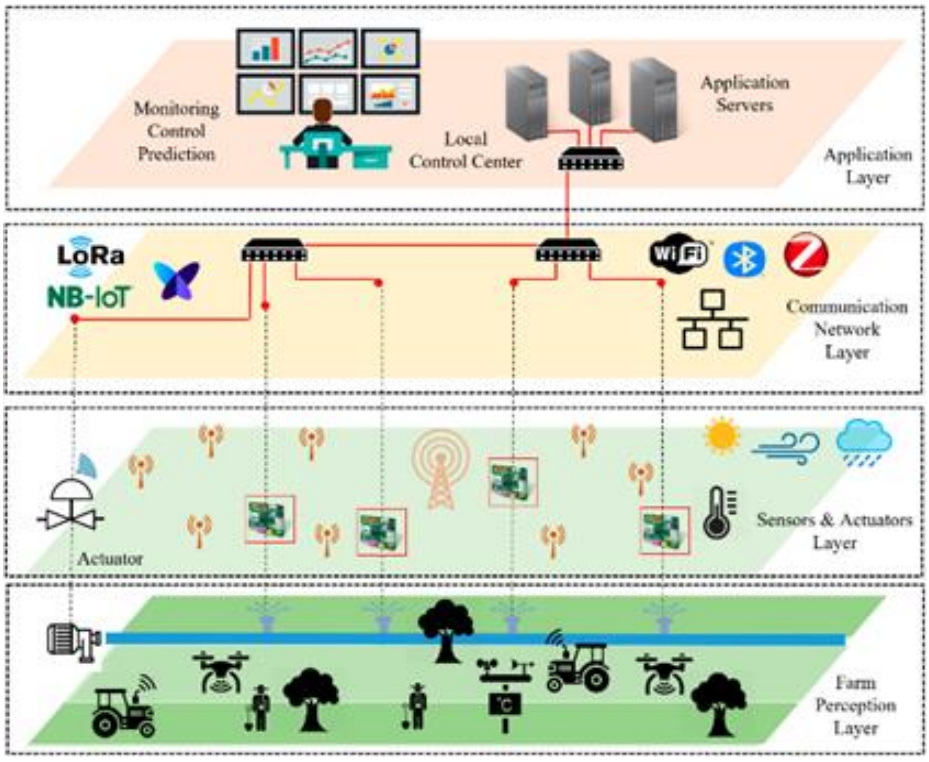


Εικόνα 2. Πολυεπίπεδη αρχιτεκτονική IoT και βασικά λειτουργικά επίπεδα σε περιβάλλον έξυπνου σπιτιού. Πηγή: (Altaie et al., 2025).

Η αρχιτεκτονική επιπέδων διευκολύνει την κατανόηση του τρόπου με τον οποίο τα δεδομένα ρέουν από τις φυσικές συσκευές προς τα ανώτερα επίπεδα επεξεργασίας. Οι Aiello et al. (2022) προτείνουν μια γενική έξυπνη αρχιτεκτονική IoT όπου το κατώτερο επίπεδο είναι το πραγματικό φυσικό επίπεδο IoT, όπου οι άνθρωποι και οι συσκευές βρίσκονται. Αυτές οι συσκευές συνδέονται μέσω πυλών (gateways) ή άμεσης αλληλεπίδρασης με ανθρώπινες συσκευές όπως τηλέφωνα και φορετές συσκευές. Οι Software Defined Gateways (SDG) και οι υπηρεσίες cloud προσπελαύνονται από τα υψηλότερα επίπεδα της αρχιτεκτονικής με ασύγχρονο τρόπο, όπου χρησιμοποιούνται ουρές μηνυμάτων που είναι αμφίδρομες.

Το ανώτερο επίπεδο της αρχιτεκτονικής είναι εκεί όπου αναδύεται η κυκλική φύση του "μέτρησε, αποφάσισε και εκτέλεσε". Τα δεδομένα από τις ουρές μηνυμάτων επεξεργάζονται για τη δημιουργία πληροφοριών πλαισίου (Aiello et al., 2022). Τα δεδομένα καθαρίζονται, συσχετίζονται και τροφοδοτούνται σε ταξινομητές για την εξαγωγή χρήσιμων πληροφοριών που μπορούν να οδηγήσουν σε ενέργειες. Η εξέλιξη από τα δεδομένα στο πλαίσιο και τις πληροφορίες συνήθως χειρίζεται από αφιερωμένους ταξινομητές που, σε ορισμένες περιπτώσεις, μπορούν να προσαρμοστούν δυναμικά στα μεταβαλλόμενα μοτίβα δεδομένων.

Στην Εικόνα 3 απεικονίζεται μια γενικευμένη πολυεπίπεδη αρχιτεκτονική IoT, η οποία περιλαμβάνει επίπεδα αντίληψης, αισθητήρων και ενεργοποιητών, επικοινωνιακά δίκτυα και επίπεδα εφαρμογών. Η αρχιτεκτονική αυτή χρησιμοποιείται σε ετερογενείς εφαρμογές IoT, όπως έξυπνα αγροτικά συστήματα και περιβάλλοντα αυτοματισμού, αναδεικνύοντας τη σημασία της ασφάλειας και της ιδιωτικότητας σε κάθε επίπεδο του συστήματος.



Εικόνα 3. Πολυεπίπεδη αρχιτεκτονική IoT με αισθητήρες, δίκτυα επικοινωνίας και επίπεδο εφαρμογών. Πηγή: (Haris et al., 2023)

2.1.3. Βασικές συσκευές IoT στα έξυπνα σπίτια

Οι συσκευές IoT που χρησιμοποιούνται στα έξυπνα σπίτια ποικίλλουν σημαντικά ως προς τη λειτουργικότητα και την εφαρμογή τους. Σύμφωνα με τους Mocrii et al. (2018), στον πυρήνα ενός συστήματος αυτοματισμού έξυπνου σπιτιού βρίσκονται συσκευές όπως έξυπνα ηχεία, θερμοστάτες, συστήματα φωτισμού, κάμερες ασφαλείας, έξυπνες κλειδαριές και έξυπνες οικιακές συσκευές. Τα έξυπνα ηχεία όπως το Amazon Echo και το Google Home λειτουργούν ως κόμβοι για τη διαχείριση έξυπνου σπιτιού, παρέχοντας επίσης επιλογές ψυχαγωγίας όπως streaming μουσικής, φωνητική αναζήτηση και εικονικούς βοηθούς.

Οι έξυπνοι θερμοστάτες και τα συστήματα ελέγχου HVAC βοηθούν τους ιδιοκτήτες να παρακολουθούν και να μειώνουν την κατανάλωση ενέργειας, με λύσεις όπως το Nest Thermostat και το Honeywell Home να προσφέρουν απομακρυσμένο έλεγχο και ρύθμιση θερμοκρασίας βασισμένη σε τεχνητή νοημοσύνη (MarketsandMarkets, 2024). Τα συστήματα ελέγχου φωτισμού, που περιλαμβάνουν έξυπνους λαμπτήρες, dimmer και αισθητήρες κίνησης, επιτρέπουν στους χρήστες να ελέγχουν τον φωτισμό από απόσταση ή να αυτοματοποιούν τον φωτισμό με βάση την παρουσία ή την ώρα της ημέρας. Τα συστήματα ασφαλείας και ελέγχου πρόσβασης, που περιλαμβάνουν έξυπνες κλειδαριές, κάμερες ασφαλείας και θυροτηλέφωνα με βίντεο, επιτρέπουν την παρακολούθηση σε πραγματικό χρόνο, την απομακρυσμένη πρόσβαση και έξυπνες ειδοποιήσεις, παρέχοντας ενισχυμένη ασφάλεια.

Η αυξανόμενη υιοθέτηση ψηφιακών βοηθών που βασίζονται σε τεχνητή νοημοσύνη καθιστά την τεχνολογία έξυπνου σπιτιού πιο διαισθητική και χωρίς χρήση χεριών. Σύμφωνα με την Grand View Research (2025), τα έξυπνα ηχεία και οι φωνητικοί βοηθοί κατέχουν κυρίαρχη θέση στην αγορά πλατφορμών έξυπνων σπιτιών, λόγω της αυξανόμενης ζήτησης των καταναλωτών για ευκολία και έλεγχο χωρίς χρήση χεριών. Οι φωνητικοί βοηθοί γίνονται όλο και περισσότερο κεντρικοί κόμβοι για την αποτελεσματική διαχείριση συνδεδεμένων συσκευών εντός πλατφορμών έξυπνων σπιτιών, με την τεχνητή νοημοσύνη να επιτρέπει στους φωνητικούς βοηθούς να μαθαίνουν τη συμπεριφορά και τις προτιμήσεις των χρηστών, με αποτέλεσμα πιο εξατομικευμένες εμπειρίες.

2.1.4. Αισθητήρες στα έξυπνα σπίτια: Τύποι και εφαρμογές

Οι αισθητήρες αποτελούν θεμελιώδη συστατικά των συστημάτων έξυπνων σπιτιών, καθώς είναι υπεύθυνοι για τη συλλογή δεδομένων από το φυσικό περιβάλλον. Ένας αισθητήρας ανιχνεύει αλλαγές στις φυσικές συνθήκες—όπως θερμοκρασία, πίεση, φως ή κίνηση—και τις μετατρέπει σε ηλεκτρικά σήματα (Puentes-Conde et al., 2025). Υπάρχουν διάφοροι τύποι αισθητήρων, ο καθένας σχεδιασμένος για συγκεκριμένες εφαρμογές: αισθητήρες θερμοκρασίας μετρούν τα επίπεδα θερμότητας και χρησιμοποιούνται σε συστήματα HVAC και βιομηχανικές διεργασίες, ενώ αισθητήρες εγγύτητας ανιχνεύουν την παρουσία κοντινών αντικειμένων χωρίς φυσική επαφή.

Σύμφωνα με μελέτη των Hammoudeh και Arioua (2018), οι αισθητήρες διαδραματίζουν κρίσιμο ρόλο σε συστήματα ανάδρασης, όπου δεδομένα πραγματικού χρόνου χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο λειτουργιών. Για παράδειγμα, σε έναν έξυπνο θερμοστάτη, ένας αισθητήρας θερμοκρασίας ανιχνεύει τις συνθήκες του δωματίου και, με βάση αυτά τα δεδομένα, το σύστημα προσαρμόζει τη θέρμανση ή την ψύξη ανάλογα. Άλλοι σημαντικοί τύποι αισθητήρων περιλαμβάνουν αισθητήρες κίνησης που χρησιμοποιούνται σε συστήματα ασφαλείας, αισθητήρες υγρασίας για τον έλεγχο της υγρασίας του αέρα, και αισθητήρες φωτός (LDR modules) που ρυθμίζουν αυτόματα τον φωτισμό με βάση τις συνθήκες φωτισμού του περιβάλλοντος.

Οι αισθητήρες παίζουν επίσης σημαντικό ρόλο στην ασφάλεια του έξυπνου σπιτιού. Οι Adhikary et al. (2024) επισημαίνουν ότι σε ένα σύστημα έξυπνου σπιτιού, διάφοροι αισθητήρες όπως οι αισθητήρες θερμοκρασίας LM35, οι αισθητήρες υπερύθρων (IR sensors) και οι αισθητήρες κίνησης χρησιμοποιούνται για την ανίχνευση της παρουσίας ή απουσίας ανθρώπινου αντικειμένου στο σπίτι και λειτουργούν ανάλογα. Επιπλέον, σύγχρονα συστήματα μπορούν να ανιχνεύουν φωτιά, επικίνδυνα αέρια και σεισμούς και να ενεργοποιούν συναγερμό, προσφέροντας μια επιπλέον στρώση ασφάλειας για τους κατοίκους.

2.1.5. Ενεργοποιητές και ο ρόλος τους στην αυτοματοποίηση

Ενώ οι αισθητήρες συλλέγουν δεδομένα, οι ενεργοποιητές (actuators) είναι υπεύθυνοι για την κίνηση ή τον έλεγχο ενός συστήματος ή μηχανισμού. Οι ενεργοποιητές μετατρέπουν ηλεκτρικά σήματα σε φυσική κίνηση ή απόκριση (Puentes-Conde et al., 2025). Οι συνήθεις τύποι περιλαμβάνουν ηλεκτρικούς ενεργοποιητές που μετατρέπουν ηλεκτρική ενέργεια σε περιστροφική ή γραμμική κίνηση, υδραυλικούς ενεργοποιητές που χρησιμοποιούν πίεση υγρού για να δημιουργήσουν μηχανική κίνηση και συχνά χρησιμοποιούνται σε βαριά μηχανήματα, και πνευματικούς ενεργοποιητές που λειτουργούν χρησιμοποιώντας πεπιεσμένο αέρα και είναι συνηθισμένοι στην αυτοματοποίηση εργοστασίων και ρομποτικά όπλα.

Σύμφωνα με τους Stolojescu-Crisan et al. (2021), σε ένα σύστημα έξυπνου σπιτιού που ονομάζεται qToggle, οι συσκευές που χρησιμοποιούνται είναι συνήθως αισθητήρες ή ενεργοποιητές με ανοδική σύνδεση δικτύου που υλοποιεί το qToggle API. Οι περισσότερες συσκευές που χρησιμοποιούνται βασίζονται σε chips ESP8266/ESP8285 ή/και σε πλακέτες Raspberry Pi. Το σύστημα επιτρέπει τη διασύνδεση αισθητήρων, ενεργοποιητών και άλλων πηγών δεδομένων με σκοπό τη δημιουργία πολλαπλών αυτοματισμών σπιτιού. Οι ενεργοποιητές λειτουργούν με βάση τις αποφάσεις που λαμβάνει ένα σύστημα ελέγχου, συχνά βασιζόμενοι σε εισόδους από αισθητήρες.

Οι ενεργοποιητές είναι απαραίτητο μέρος των σύγχρονων συστημάτων έξυπνων σπιτιών καθώς επιτρέπουν στους χρήστες να λειτουργούν από απόσταση διάφορο εξοπλισμό σύμφωνα με τις ανάγκες τους (IEEE BLP, 2024). Αυτά περιλαμβάνουν συστήματα θέρμανσης, φώτα, θερμοστάτες και συστήματα ασφαλείας. Για παράδειγμα, όταν ένας αισθητήρας φωτισμού ανιχνεύει ότι ένα δωμάτιο είναι σκοτεινό, ένας ενεργοποιητής μπορεί να ενεργοποιήσει το σύστημα φωτισμού για να ρυθμίσει τη φωτεινότητα του δωματίου. Η ενσωμάτωση αισθητήρων και ενεργοποιητών δημιουργεί έναν βρόχο ελέγχου που επιτρέπει την αυτόνομη λειτουργία των συστημάτων έξυπνων σπιτιών.

2.1.6. Πρωτόκολλα επικοινωνίας στα έξυπνα σπίτια

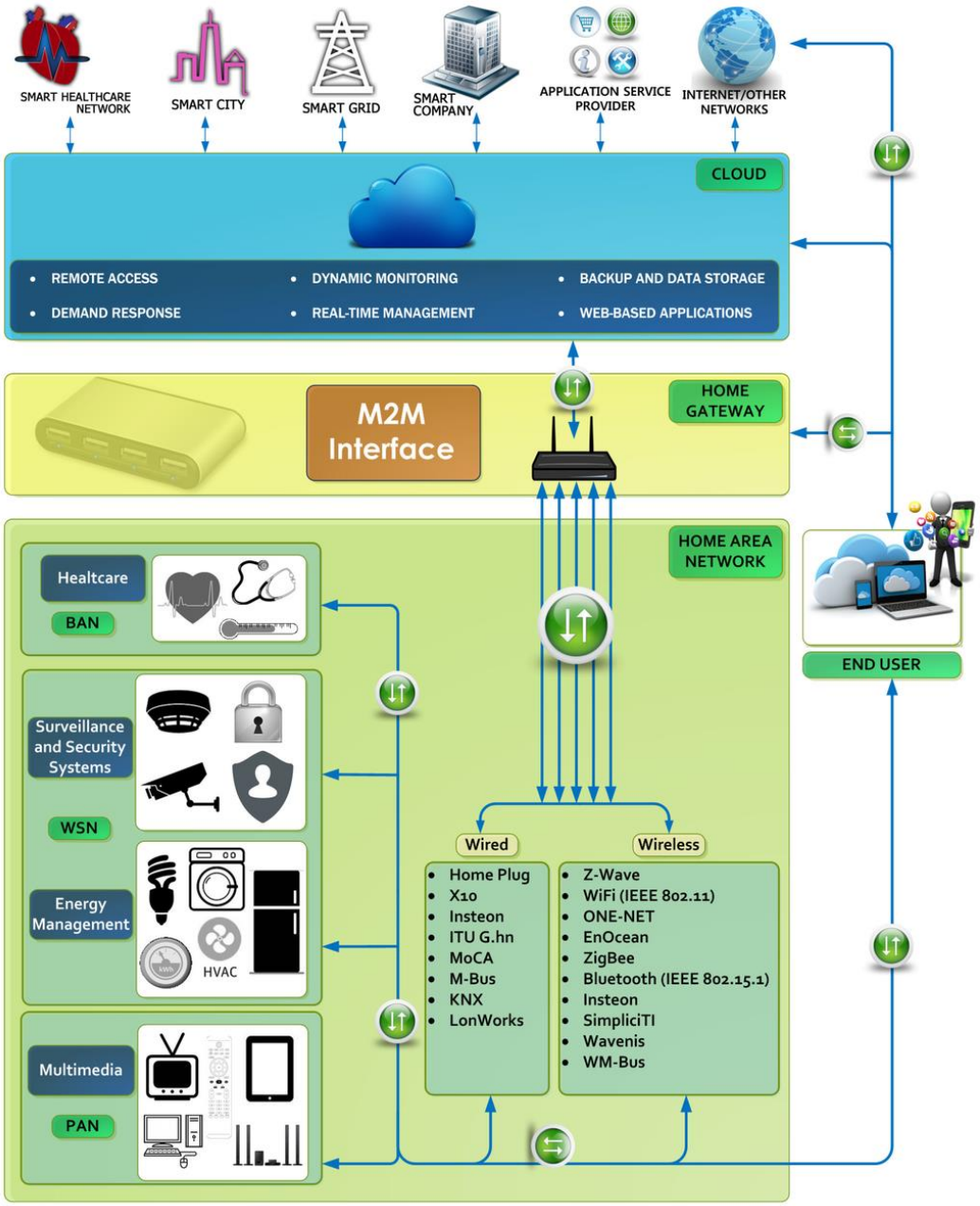
Τα πρωτόκολλα επικοινωνίας καθορίζουν τον τρόπο με τον οποίο οι συσκευές και οι αισθητήρες μπορούν να επικοινωνούν μεταξύ τους σε ένα περιβάλλον έξυπνου σπιτιού. Σύμφωνα με τους Schulz & Scilla, (2024), κεντρικής σημασίας στην συζήτηση για τα έξυπνα σπίτια είναι ο τρόπος με τον οποίο οι διάφορες συσκευές επικοινωνούν, λειτουργούν και ενσωματώνονται. Το ZigBee είναι ένας από τους κορυφαίους παίκτες στην αγορά έξυπνων σπιτιών, παρέχοντας mesh συνδεσιμότητα χαμηλής ισχύος και χαμηλού εύρους ζώνης τόσο για εφαρμογές αυτοματισμού σπιτιού όσο και για διαχείριση ενέργειας.

Το Wi-Fi αποτελεί το πιο διαδεδομένο πρωτόκολλο επικοινωνίας για συσκευές IoT λόγω της υψηλής ταχύτητας και της ευρείας διαθεσιμότητας σε οικιακά περιβάλλοντα. Το Wi-Fi επιτρέπει σε συσκευές όπως smartphones, tablets, smart TVs και συσκευές έξυπνου σπιτιού να δημιουργήσουν ασύρματη σύνδεση σε ένα τοπικό δίκτυο (LAN) ή στο διαδίκτυο (Lopez et al., 2016). Το Bluetooth και ειδικότερα το Bluetooth Low Energy (BLE) χρησιμοποιείται για συσκευές που απαιτούν χαμηλή κατανάλωση ενέργειας και λειτουργούν σε κοντινές αποστάσεις, όπως φορετές συσκευές και έξυπνες κλειδαριές. Το Z-Wave είναι ένα μη-IP πρωτόκολλο mesh που χρησιμοποιεί υπο-GHz ISM ζώνες και εστιάζει σε συσκευές χαμηλού εύρους ζώνης που απαιτούν χαμηλή ισχύ και αξιόπιστη επικοινωνία, όπως συστήματα ασφαλείας, αισθητήρες, διακόπτες και κλειδαριές (Sikdar, 2024).

Στην Εικόνα 4 αποτυπώνεται μια ολοκληρωμένη αρχιτεκτονική επικοινωνίας έξυπνου σπιτιού, όπου συνυπάρχουν ενσύρματα και ασύρματα δίκτυα, πύλες οικιακής διασύνδεσης (home gateways) και υπηρεσίες cloud. Η εικόνα αναδεικνύει τον ρόλο των M2M διεπαφών στη διασύνδεση αισθητήρων, συστημάτων ασφάλειας, διαχείρισης ενέργειας και πολυμέσων με εξωτερικά δίκτυα και παρόχους υπηρεσιών, υποστηρίζοντας λειτουργίες απομακρυσμένης πρόσβασης, παρακολούθησης και αποθήκευσης δεδομένων.

Πρόσφατα, το πρωτόκολλο Matter έχει αναδυθεί ως μια πρότυπη λύση για τη βελτίωση της διαλειτουργικότητας μεταξύ διαφορετικών κατασκευαστών. Το Matter είναι ένα ανοιχτό πρότυπο που στοχεύει να κάνει αυτές τις συσκευές να λειτουργούν καλύτερα μαζί, χρησιμοποιώντας το πρωτόκολλο Internet Protocol (IP), βελτιώνοντας τη

συμβατότητα και την ασφάλεια (Intuz, 2024). Το Matter υποστηρίζει εγγενώς Wi-Fi, Ethernet και το ασύρματο mesh δίκτυο Thread. Ενώ το Matter υποστηρίζει εγγενώς Wi-Fi, Ethernet και Thread, ο στόχος του είναι να απλοποιήσει τα έξυπνα σπίτια, συμπεριλαμβανομένων εκείνων που διαθέτουν ήδη συσκευές που χρησιμοποιούν άλλες τεχνολογίες δικτύωσης, όπως Zigbee ή Z-Wave.



Εικόνα 4. Ολοκληρωμένη αρχιτεκτονική επικοινωνίας και διασύνδεσης συσκευών σε περιβάλλον έξυπνου σπιτιού με υποστήριξη cloud και M2M διεπαφών. Πηγή: (Mendes et al., 2015).

2.1.7. Πλατφόρμες και κόμβοι ελέγχου έξυπνων σπιτιών

Οι πλατφόρμες αυτοματισμού σπιτιού λειτουργούν ως το κεντρικό λογισμικό ελέγχου για τους έξυπνους κόμβους, παρέχοντας μια διαδραστική διεπαφή χρήστη για την παρακολούθηση και τον έλεγχο όλων των συσκευών (Dusun IoT, 2024). Οι πλατφόρμες αυτές δίνουν τη δυνατότητα στους χρήστες να δημιουργήσουν αυτοματισμούς, σκηνές, ρουτίνες και προγράμματα, παρέχοντας πλήρη έλεγχο στο οικοσύστημα του έξυπνου σπιτιού. Η επιλογή της κατάλληλης πλατφόρμας αυτοματισμού σπιτιού είναι κρίσιμη καθώς καθορίζει τη συνολική εμφάνιση και λειτουργικότητα του έξυπνου σπιτιού.

Οι κορυφαίες πλατφόρμες περιλαμβάνουν την Amazon Alexa, το Google Home, το Apple HomeKit και το Samsung SmartThings, οι οποίες όλες υποστηρίζουν το Matter, που σημαίνει ότι μπορείτε να χρησιμοποιήσετε οποιαδήποτε από τις εφαρμογές τους, έξυπνα ηχεία, κόμβους και έξυπνους φωνητικούς βοηθούς για να διαχειριστείτε τις συσκευές Matter (Alicia, 2024). Το Samsung SmartThings Station έχει μετατραπεί σε έναν ισχυρό κόμβο έξυπνου σπιτιού με πιστοποίηση Matter, αποτελώντας ένα μεγάλο βήμα από τους απλούστερους κόμβους καθώς θα ελέγχει σχεδόν κάθε προϊόν με πιστοποίηση Matter και είναι πολύ εύκολο στη χρήση (Patterson, 2025).

Η απόφαση μεταξύ ενός κόμβου ελεγχόμενου τοπικά και ενός κόμβου διαχειριζόμενου από το cloud εξαρτάται από τις ατομικές προτιμήσεις και συγκεκριμένες περιπτώσεις χρήσης (Dusun IoT, 2024). Οι τοπικά ελεγχόμενοι κόμβοι προσφέρουν καλύτερη απόκριση και ιδιωτικότητα καθώς τα δεδομένα παραμένουν εντός του τοπικού δικτύου, ενώ οι κόμβοι που βασίζονται στο cloud παρέχουν απομακρυσμένη πρόσβαση από οπουδήποτε στον κόσμο και συχνά περιλαμβάνουν προηγμένες λειτουργίες τεχνητής νοημοσύνης. Η τάση προς υβριδικές λύσεις που συνδυάζουν τοπικό και cloud έλεγχο γίνεται όλο και πιο δημοφιλής, προσφέροντας το καλύτερο και των δύο κόσμων.

2.1.8. Μικροελεγκτές και πλατφόρμες ανάπτυξης

Οι μικροελεγκτές αποτελούν τον εγκέφαλο των συσκευών IoT, επιτρέποντας τη συλλογή, επεξεργασία και μετάδοση δεδομένων. Αυτές οι μικρές πλακέτες ανάπτυξης συνδέονται με διάφορες συσκευές εντός του σπιτιού για να επιτρέψουν την αυτοματοποίηση και τον έλεγχο. Σύμφωνα με τους Ezugwu et al. (2025), υπάρχουν

διάφοροι τύποι πλακετών μικροελεγκτών που χρησιμοποιούνται στην ανάπτυξη έξυπνων σπιτιών και οι κύριοι περιγράφονται παρακάτω. Η πλακέτα ESP8266 είναι ένας δημοφιλής μικροελεγκτής και πλακέτα που χρησιμοποιείται στην αυτοματοποίηση σπιτιού, γνωστή για την οικονομική της αποδοτικότητα, την ελάχιστη χρήση ενέργειας και την ευκολία χρήσης. Οι ενότητες ESP8266 μπορούν να λειτουργήσουν ως αυτόνομες συσκευές χωρίς την ανάγκη για πρόσθετους μικροελεγκτές ή ενότητες Wi-Fi, παρέχοντας δυνατότητες IoT με ενσωματωμένη συνδεσιμότητα Wi-Fi.

Το Raspberry Pi είναι ένας υπολογιστής που έρχεται σε σχεδιασμό μονής πλακέτας, αναπτυγμένος από το Raspberry Pi Foundation (Ezugwu et al., 2025). Χρησιμοποιείται ευρέως ως μικρή και οικονομική πλακέτα υπολογιστή σε διάφορες εφαρμογές, συμπεριλαμβανομένης της συγκέντρωσης δεδομένων, των πυλών συσκευών και των κόμβων στα έξυπνα σπίτια. Το Arduino UNO είναι μια άλλη δημοφιλής πλατφόρμα που χρησιμοποιείται για την ανάπτυξη πρωτοτύπων συστημάτων έξυπνων σπιτιών, προσφέροντας ευκολία προγραμματισμού και ευελιξία στην ενσωμάτωση με διάφορους αισθητήρες και ενεργοποιητές.

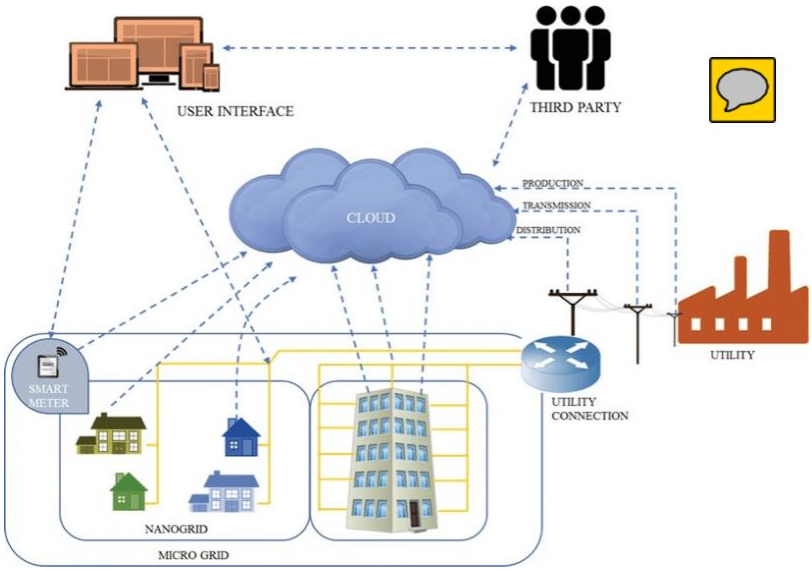
Η επιλογή της κατάλληλης πλατφόρμας ανάπτυξης εξαρτάται από τις απαιτήσεις του έργου, συμπεριλαμβανομένων παραγόντων όπως η υπολογιστική ισχύς, η κατανάλωση ενέργειας, η συνδεσιμότητα δικτύου και το κόστος. Σύμφωνα με τους Stolojescu-Crisan et al. (2021), η ενότητα Wi-Fi ESP8266 αντιπροσωπεύει ένα σύνολο αποδοτικών και ιδιαίτερα ενσωματωμένων ασύρματων συστημάτων σε chip (SoCs), τα οποία παρέχουν μια πλήρη και αυτόνομη λύση δικτύου Wi-Fi. Η έκδοση ESP8266EX είναι ένα από τα πιο ενσωματωμένα chip Wi-Fi στη βιομηχανία, ενσωματώνοντας μια βελτιωμένη έκδοση του επεξεργαστή L106 Diamond series 32-bit από την Tensilica, με on-chip SRAM.

2.1.9. Συστήματα διαχείρισης ενέργειας και βιωσιμότητα

Η ενεργειακή αποδοτικότητα αποτελεί έναν από τους κύριους λόγους για τους οποίους οι καταναλωτές υιοθετούν τεχνολογίες έξυπνων σπιτιών. Τα έξυπνα συστήματα διαχείρισης ενέργειας περιλαμβάνουν έξυπνους θερμοστάτες, συστήματα παρακολούθησης ενέργειας και έξυπνες πρίζες που επιτρέπουν στους χρήστες να παρακολουθούν και να βελτιστοποιούν την κατανάλωση ενέργειας. Σύμφωνα με τον

Dąbrowska (2024), ανάλογα με το επίπεδο αυτοματοποίησης του σπιτιού σας, μπορείτε να μειώσετε τους λογαριασμούς σας μεταξύ 5% και 22%, ενώ η τεχνολογία συνεχίζει να εξελίσσεται, πράγμα που σημαίνει ότι αυτά τα ποσοστά μπορούν ακόμα να αυξηθούν.

Στην Εικόνα 5 παρουσιάζεται μια αρχιτεκτονική έξυπνης ενεργειακής διαχείρισης, όπου έξυπνοι μετρητές, οικιακά και μικροδίκτυα (microgrids) επικοινωνούν με cloud υποδομές και παρόχους ενέργειας. Η εικόνα αναδεικνύει τον ρόλο των δεδομένων κατανάλωσης στη βελτιστοποίηση της ενεργειακής απόδοσης, αλλά και τους κινδύνους ιδιωτικότητας που προκύπτουν από τη συλλογή και διαβίβαση λεπτομερών πληροφοριών σχετικά με τις συνήθειες των χρηστών.



Εικόνα 5. Αρχιτεκτονική έξυπνων ενεργειακών δικτύων με χρήση IoT, cloud και διασύνδεση παρόχων ενέργειας. Πηγή: (Haris et al., 2023)

Οι πλατφόρμες που προσφέρουν ρουτίνες βασισμένες σε τεχνητή νοημοσύνη ικανές να μαθαίνουν τα προγράμματα των χρηστών μπορούν να εξοικονομήσουν έως και 30% στους ετήσιους λογαριασμούς ενέργειας, όπως αναφέρθηκε από τη Statista στην έρευνά τους του 2024 για τη διαχείριση οικιακής ενέργειας (Magara & Zhou, 2024). Τα έξυπνα συστήματα φωτισμού, που χρησιμοποιούν αισθητήρες κίνησης και φυσικού φωτός, μπορούν να μειώσουν σημαντικά την κατανάλωση ενέργειας

απενεργοποιώντας αυτόματα τα φώτα όταν δεν χρησιμοποιούνται. Επίσης, τα συστήματα παρακολούθησης ενέργειας παρέχουν λεπτομερείς πληροφορίες σχετικά με τη χρήση ενέργειας κάθε συσκευής, επιτρέποντας στους χρήστες να εντοπίσουν και να μειώσουν την κατανάλωση σε περιοχές υψηλής κατανάλωσης.

Η ενσωμάτωση ανανεώσιμων πηγών ενέργειας, όπως ηλιακών πάνελ, με συστήματα έξυπνων σπιτιών γίνεται επίσης όλο και πιο συνηθισμένη. Συστήματα που συνδυάζουν φωτοβολταϊκή τεχνολογία και IoT σε ένα έξυπνο σπίτι μπορούν να αυξήσουν την ενεργειακή απόδοση και να υποστηρίξουν προσπάθειες περιβαλλοντικής διατήρησης (Stolojescu-Crisan et al., 2021). Εάν η ηλιακή τάση είναι ανεπαρκής, το σύστημα θα απενεργοποιήσει μη απαραίτητο εξοπλισμό ή θα μειώσει την κατανάλωση ενέργειας, ενώ οι χρήστες μπορούν να ελέγχουν το σύστημα μέσω smartphone για να ενεργοποιήσουν οικιακές συσκευές όπως χρειάζεται.

2.1.10. Ασφάλεια και διαχείριση δεδομένων στα IoT

Η ασφάλεια και η ιδιωτικότητα αποτελούν κρίσιμες προκλήσεις στα συστήματα έξυπνων σπιτιών λόγω του μεγάλου όγκου ευαίσθητων δεδομένων που συλλέγονται και μεταδίδονται. Σύμφωνα με τους Magara et al. (2024), το IoT αντιμετωπίζει σοβαρές προκλήσεις ιδιωτικότητας και ασφάλειας, που περιλαμβάνουν περίπλοκα ζητήματα όπως η απόκτηση δεδομένων, η ανωνυμοποίηση, η διατήρηση, οι πρακτικές κοινής χρήσης και η συμπεριφορική κατάταξη σε προφίλ. Η αποτελεσματική αντιμετώπιση αυτών των προκλήσεων απαιτεί την ανάπτυξη επεκτάσιμων λύσεων, καινοτόμων στρατηγικών διαχείρισης και προσαρμόσιμων πλαισίων πολιτικής.

Τα υπάρχοντα μέτρα ασφάλειας και πρωτόκολλα για την προστασία των συσκευών και δικτύων IoT έχουν εξελιχθεί για να αντιμετωπίσουν τις μοναδικές προκλήσεις που θέτει η ευρείας κλίμακας ανάπτυξη συσκευών IoT (Magara et al., 2024). Αυτά περιλαμβάνουν κρυπτογράφηση από άκρο σε άκρο, πιστοποίηση συσκευών και ενσωμάτωση cloud. Με τα συσκευές IoT, εναπόκειται στους χρήστες να διασφαλίσουν ότι προστατεύονται επαρκώς από μέτρα ασφάλειας όπως ισχυροί κωδικοί πρόσβασης, ενημερώσεις λογισμικού και κρυπτογράφηση (Dąbrowska, 2024). Επιπλέον, ο διαχωρισμός του δικτύου, όπου οι συσκευές IoT απομονώνονται από άλλες κρίσιμες συσκευές στο δίκτυο, μπορεί να μειώσει τους κινδύνους που σχετίζονται με πιθανές παραβιάσεις ασφαλείας.

2.1.11. Διαλειτουργικότητα και πρότυπα

Η διαλειτουργικότητα IoT αναφέρεται στην ικανότητα των συστημάτων να επικοινωνούν και να συνεργάζονται απρόσκοπτα σε διάφορες συσκευές και πλατφόρμες IoT (Magara et al., 2024). Είναι απαραίτητη για την επιτυχία και την ευρεία υιοθέτηση του Διαδικτύου των Πραγμάτων. Η επίτευξη διαλειτουργικότητας παρουσιάζεται με προκλήσεις αλλά και σημαντικά οφέλη. Ένα από τα μεγαλύτερα προβλήματα με τα έξυπνα σπίτια είναι η έλλειψη συμβατότητας μεταξύ συσκευών και κόμβων, ακόμα και όταν η συμβατότητα χρησιμοποιείται ως πλεονέκτημα πώλησης, μπορούν να προκύψουν προβλήματα (Cawley, 2024).

Οι προσπάθειες τυποποίησης της τεχνολογίας έξυπνου σπιτιού, όπως το πρωτόκολλο Matter της Connectivity Standards Alliance, βρίσκονται σε εξέλιξη (Prashanth et al., 2025). Αυτό θα βελτιώσει τη διαλειτουργικότητα μεταξύ διαφορετικών συσκευών και μαρκών, καθιστώντας ευκολότερο για τους καταναλωτές να δημιουργήσουν και να διαχειριστούν τα έξυπνα σπίτια τους. Προϊόντα με καλύτερη πιθανότητα διαλειτουργικότητας είναι εκείνα που ακολουθούν ένα κοινό πρότυπο ή πρωτόκολλο, όπως το Zigbee και το Z-Wave που είναι δύο κοινά ασύρματα πρότυπα για την κατασκευή συστημάτων αυτοματισμού σπιτιού (Dąbrowska, 2024).

2.1.12. Μελλοντικές τάσεις και εξελίξεις

Το μέλλον των έξυπνων σπιτιών είναι εξαιρετικά πολλά υποσχόμενο, με συνεχείς εξελίξεις στο IoT και την τεχνητή νοημοσύνη να οδηγούν την καινοτομία. Η τεχνητή νοημοσύνη γίνεται πιο εξελιγμένη, επιτρέποντας εξυπνότερη αυτοματοποίηση και εξατομίκευση ((Prashanth et al., 2025). Τα μελλοντικά έξυπνα σπίτια θα προβλέπουν τις ανάγκες των χρηστών, μαθαίνοντας ρουτίνες και προτιμήσεις για να παρέχουν μια πραγματικά διαισθητική εμπειρία διαβίωσης. Καθώς οι συσκευές έξυπνου σπιτιού συλλέγουν περισσότερα δεδομένα, η ιδιωτικότητα και η ασφάλεια είναι υψίστης σημασίας, με κατασκευαστές να επενδύουν σε ισχυρή κρυπτογράφηση και μέτρα ασφαλείας για την προστασία των πληροφοριών των χρηστών.

Η ανάπτυξη της τεχνολογίας 5G αναμένεται να επιταχύνει περαιτέρω την υιοθέτηση έξυπνων συσκευών, παρέχοντας ταχύτερη μετάδοση δεδομένων με χαμηλή καθυστέρηση. Σύμφωνα με την Grand View Research (2024), η τεχνολογία 5G παρέχει

ταχύτερη μετάδοση δεδομένων με χαμηλή καθυστέρηση, επιτρέποντας απρόσκοπτη επικοινωνία μεταξύ συσκευών. Το edge computing ενισχύει την επεξεργασία δεδομένων σε πραγματικό χρόνο σε επίπεδο συσκευής, ενώ η τεχνητή νοημοσύνη και η μηχανική μάθηση επιτρέπουν προγνωστική ανάλυση και αυτοματοποίηση σε διάφορους κλάδους. Αυτή η τάση αναμένεται να οδηγήσει στην επέκταση της βιομηχανίας συσκευών IoT τα επόμενα χρόνια.

Η ενσωμάτωση της τεχνολογίας συλλογής ενέργειας, όπως αισθητήρων χωρίς μπαταρία που τροφοδοτούνται από κινητική ή ηλιακή ενέργεια, αναμένεται να ξεπεράσει τα 108 εκατομμύρια μονάδες αποστολών φέτος, οδηγώντας την υιοθέτηση σε βιώσιμη κατασκευή και αναβαθμίσεις (Magara & Zhou, 2024). Επιπλέον, η τεχνολογία Ultra-Wideband (UWB) για χωρική επίγνωση προσφέρει ακριβή ανίχνευση τοποθεσίας με ακρίβεια 10-30 εκατοστών, ενισχύοντας την πρόληψη κλοπής και την αυτοματοποίηση ασφάλειας. Αυτές οι τεχνολογικές εξελίξεις υπόσχονται να δημιουργήσουν πιο έξυπνα, αποδοτικά και ασφαλή οικιακά περιβάλλοντα στο μέλλον.

2.2. Αρχές κυβερνοασφάλειας και ιδιωτικότητας στα έξυπνα συστήματα

2.2.1. Εισαγωγή στις αρχές ασφάλειας και ιδιωτικότητας

Η κυβερνοασφάλεια και η προστασία της ιδιωτικότητας αποτελούν θεμελιώδεις πυλώνες για την ασφαλή λειτουργία των έξυπνων συστημάτων σπιτιών. Καθώς το Διαδίκτυο των Πραγμάτων συνεχίζει να επαναπροσδιορίζει τον τρόπο με τον οποίο αλληλεπιδρούμε με τους χώρους διαβίωσής μας, η ασφάλεια των έξυπνων σπιτιών έχει γίνει ολοένα και πιο επιτακτική (Vardakis et al., 2024). Τα έξυπνα σπίτια ενσωματώνουν πολυάριθμες συσκευές και εφαρμογές για τη βελτίωση της συνολικής ποιότητας ζωής, καθιστώντας τα συστήματα αυτά στόχους υψηλής αξίας για κυβερνοεπιθέσεις. Σύμφωνα με τους Ali & Awad, (2018), η εφαρμογή του μοντέλου IoT στα έξυπνα σπίτια, συνδέοντας αντικείμενα στο Διαδίκτυο, θέτει νέες προκλήσεις ασφάλειας και ιδιωτικότητας όσον αφορά την εμπιστευτικότητα, την αυθεντικότητα και την ακεραιότητα των δεδομένων που αισθάνονται, συλλέγονται και ανταλλάσσονται τα αντικείμενα IoT.

Η τρέχουσα κατάσταση της ασφάλειας στα έξυπνα σπίτια παρουσιάζει σημαντικές αδυναμίες. Οι Magara et al. (2024) επισημαίνουν ότι η συλλογή και επεξεργασία δεδομένων χρηστών σε περιβάλλοντα έξυπνων σπιτιών στερούνται διαφάνειας και ελέγχου, όπως συμβαίνει και με άλλες συσκευές IoT. Τα έξυπνα σπίτια λειτουργούν εντός του σπιτιού, ενός χώρου που είναι τόσο ηθικά όσο και νομικά ιδιαίτερα προστατευμένος και χαρακτηρίζεται από μια σιωπηρή προσδοκία ιδιωτικότητας από την πλευρά του χρήστη. Οι προκλήσεις αυτές καθιστούν τα έξυπνα σπίτια εξαιρετικά ευάλωτα σε διαφορετικούς τύπους επιθέσεων ασφαλείας, με αποτέλεσμα τα έξυπνα σπίτια βασισμένα σε IoT να είναι ανασφαλή.

2.2.2. Θεμελιώδεις αρχές κυβερνοασφάλειας

Οι θεμελιώδεις αρχές κυβερνοασφάλειας για τα έξυπνα συστήματα βασίζονται στην τριάδα CIA: Εμπιστευτικότητα (Confidentiality), Ακεραιότητα (Integrity) και Διαθεσιμότητα (Availability). Οι Abdullah et al., (2019) τονίζουν ότι τα συστήματα πληροφοριών IoT πρέπει να διασφαλίζουν ότι τα δεδομένα παραμένουν εμπιστευτικά, ακέραια και διαθέσιμα σε εξουσιοδοτημένους χρήστες. Η εμπιστευτικότητα διασφαλίζει ότι τα δεδομένα είναι προσβάσιμα μόνο σε εξουσιοδοτημένα άτομα ή συστήματα, προστατεύοντας ευαίσθητες πληροφορίες από μη εξουσιοδοτημένη πρόσβαση. Η ακεραιότητα εγγυάται ότι τα δεδομένα δεν έχουν τροποποιηθεί ή αλλοιωθεί κατά τη μετάδοση ή αποθήκευση, ενώ η διαθεσιμότητα εξασφαλίζει ότι τα συστήματα και τα δεδομένα είναι προσβάσιμα όταν χρειάζονται.

Πέραν της τριάδας CIA, σύγχρονες προσεγγίσεις ασφάλειας για έξυπνα σπίτια ενσωματώνουν πρόσθετες αρχές όπως η αυθεντικοποίηση και η μη αποποίηση ευθύνης. Σύμφωνα με τους Aldahmani et al., (2023), οι αρχές αυτές αποτελούν κρίσιμα στοιχεία για την κατασκευή ασφαλών συστημάτων IoT που μπορούν να αντισταθούν σε σύγχρονες κυβερνοαπειλές. Η αυθεντικοποίηση επαληθεύει την ταυτότητα των χρηστών και των συσκευών πριν από την παροχή πρόσβασης στο σύστημα, ενώ η μη αποποίηση ευθύνης διασφαλίζει ότι οι ενέργειες που εκτελούνται δεν μπορούν να αρνηθούν από τον εκτελεστή αργότερα. Αυτές οι αρχές είναι ιδιαίτερα σημαντικές σε περιβάλλοντα έξυπνων σπιτιών όπου πολλαπλές συσκευές και χρήστες αλληλεπιδρούν συνεχώς.

2.2.3. Κρυπτογράφηση και προστασία δεδομένων

Η κρυπτογράφηση αποτελεί το ισοδύναμο μιας ασφαλούς κλειδαριάς για τα δεδομένα στην ψηφιακή εποχή. Οι συσκευές έξυπνου σπιτιού που χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο εξασφαλίζουν ότι τα δεδομένα μετατρέπονται σε ασφαλή κώδικα από τη στιγμή που εγκαταλείπουν τη συσκευή μέχρι να φτάσουν στον προορισμό τους (Integrated Media Systems, 2024). Αυτό σημαίνει ότι ακόμη και αν τα δεδομένα παρεμποδιστούν κατά τη μετάδοση, παραμένουν μη αναγνώσιμα σε οποιονδήποτε χωρίς το σωστό κλειδί αποκρυπτογράφησης. Τα ασφαλή πρωτόκολλα επικοινωνίας, όπως το SSL/TLS, παρέχουν πρόσθετα επίπεδα προστασίας, διασφαλίζοντας ότι το ψηφιακό αποτύπωμα προστατεύεται από αδιάκριτα βλέμματα.

Η υλοποίηση ισχυρών μεθόδων κρυπτογράφησης για τη μετάδοση και αποθήκευση δεδομένων αποτελεί κρίσιμη αντιμετώπιση των κινδύνων που σχετίζονται με τις έξυπνες συσκευές. Οι Vardakis et al., (2024) προτείνουν την εφαρμογή ισχυρών μεθόδων κρυπτογράφησης για τη μετάδοση και αποθήκευση δεδομένων που συλλέγονται από συσκευές IoT, συμπεριλαμβανομένης της χρήσης πολυπαραγοντικής αυθεντικοποίησης ή ακόμη και βιομετρικών δεδομένων για τον περιορισμό της πρόσβασης στη συσκευή. Επιπλέον, ο Advanced Encryption Standard (AES) έχει γίνει ευρέως αποδεκτός ως το πρότυπο κρυπτογράφησης για συσκευές IoT λόγω της ισχυρής ασφάλειας και της αποδοτικότητάς του σε συσκευές με περιορισμένους πόρους.

2.2.4. Μηχανισμοί αυθεντικοποίησης και έλεγχος πρόσβασης

Η αυθεντικοποίηση αποτελεί θεμελιώδη μηχανισμό ασφάλειας για τα συστήματα έξυπνων σπιτιών. Για την εξουσιοδότηση συσκευών IoT σε έξυπνα σπίτια, πρέπει να χρησιμοποιούνται πολλαπλά μέτρα ασφάλειας όπως κωδικοί πρόσβασης, κωδικοί ή έξυπνες κάρτες για την αυθεντικοποίηση της ταυτότητας του ιδιοκτήτη (Ghazali & Zakaria, 2018). Παρόλο που η αυθεντικοποίηση δεν προστατεύει 100% από την εκμετάλλευση, μπορεί να έχει πλεονεκτήματα στην επέκταση του κύκλου ζωής των συσκευών και να λειτουργήσει ως αποτρεπτικό μέσο για τους εγκληματίες του κυβερνοχώρου. Ως αποτέλεσμα, η διαδικασία αυθεντικοποίησης προσφέρει ένα συμπληρωματικό επίπεδο πολυπλοκότητας ασφάλειας που μπορεί να ενισχύσει την προστασία.

Οι σύγχρονες προσεγγίσεις αυθεντικοποίησης για έξυπνα σπίτια περιλαμβάνουν ελαφρά σχήματα κατάλληλα για συσκευές με περιορισμένους πόρους. Οι Asghar et al., (2023) προτείνουν ένα ισχυρό και αποδοτικό σχήμα αυθεντικοποίησης χρήστη για να αντιμετωπίσουν επιθέσεις συλλήψης κόμβων σε έξυπνα σπίτια. Κατά τη φάση αυθεντικοποίησης, οι μυστικές παράμετροι του κινητού χρήστη δεν προωθούνται σε μηνύματα που ανταλλάσσονται, αλλά αντ' αυτού κρυπτογραφούν τις παραμέτρους που ανταλλάσσονται μέσω του δημόσιου καναλιού μαζί με έναν τυχαίο αριθμό. Εάν μια παραβιασμένη έξυπνη συσκευή επιχειρήσει να υπολογίσει τις μυστικές παράμετρους του χρήστη, θα αποτύχει να εξαγάγει οποιαδήποτε σχετική πληροφορία, εμποδίζοντας έτσι την απόκρυψη ταυτότητας.

2.2.5. Αρχές προστασίας ιδιωτικότητας στα IoT

Η προστασία της ιδιωτικότητας στα έξυπνα σπίτια περιλαμβάνει περίπλοκα ζητήματα όπως η απόκτηση δεδομένων, η ανωνυμοποίηση, η διατήρηση, οι πρακτικές κοινής χρήσης και η συμπεριφορική κατάταξη σε προφίλ. Οι Magara et al. (2024) τονίζουν ότι τα προβλήματα ιδιωτικότητας στο IoT είναι αλληλένδετα με ένα πλέγμα ζητημάτων εξουσιοδότησης, διλημμάτων ανωνυμοποίησης, πολυπλοκότητας διατήρησης δεδομένων, διλημμάτων κοινής χρήσης δεδομένων και παραδόξων προφίλ. Καθώς πλοηγούμαστε μέσα από αυτό το επικίνδυνο έδαφος, γίνεται σαφές ότι η ιδιωτικότητα είναι περισσότερο από ένα νομοθετικό ζήτημα· είναι άρρηκτα συνδεδεμένη με τον υποκείμενο ιστό της λειτουργίας IoT.

Η προσέγγιση "Privacy by Design" (PbD) ορίζεται ως μια δημοφιλής προσέγγιση που επιτρέπει την ενσωμάτωση της ιδιωτικότητας στον σχεδιασμό των συστημάτων πληροφοριών και των επιχειρηματικών διαδικασιών, διασφαλίζοντας ότι η ιδιωτικότητα λαμβάνεται υπόψη πριν και καθ' όλη τη διάρκεια της ανάπτυξης και υλοποίησης όλων των πρωτοβουλιών που αφορούν προσωπικές πληροφορίες (Dasgupta et al., 2019). Η Dr. Ann Cavoukian την πρότεινε για πρώτη φορά στον Καναδά στη δεκαετία του 1990, και το PbD είναι μία από τις ιδιαίτερα συνιστώμενες προσεγγίσεις για την προστασία των ανησυχιών ιδιωτικότητας του ατόμου στο IoT. Δυστυχώς, παρόλο που η Ομοσπονδιακή Επιτροπή Εμπορίου των ΗΠΑ (FTC) και η Ευρωπαϊκή Επιτροπή αποδέχτηκαν ότι το PbD είναι αποτελεσματικό, δεν όλοι οι

κατασκευαστές το λαμβάνουν υπόψη κατά την ανάπτυξη συσκευών και εφαρμογών IoT.

2.2.6. Ελαχιστοποίηση δεδομένων και ανωνυμοποίηση

Η αρχή της ελαχιστοποίησης δεδομένων επιβάλλει τη συλλογή μόνο των δεδομένων που είναι απαραίτητα για τον προβλεπόμενο σκοπό. Οι Bentotahewa et al., (2022) υποστηρίζουν ότι οι συσκευές IoT είναι εγγενείς στην καθημερινή μας ζωή, συλλέγοντας συνεχώς δεδομένα για τη βελτίωση των εμπειριών των χρηστών, από περιβαλλοντικούς αισθητήρες σε έξυπνα σπίτια που παρακολουθούν τη θερμοκρασία και την υγρασία έως φορετές συσκευές που παρακολουθούν μετρήσεις υγείας όπως ο καρδιακός ρυθμός και τα πρότυπα ύπνου. Ωστόσο, υπάρχει σημαντική ανησυχία σχετικά με τη διαφάνεια με την οποία αυτά τα δεδομένα χειρίζονται. Οι χρήστες συχνά χρειάζονται σαφείς πληροφορίες σχετικά με το πώς χρησιμοποιούνται τα δεδομένα τους, με ποιους μοιράζονται ή πώς προστατεύονται.

Η ανωνυμοποίηση αποτελεί ένα κρίσιμο εργαλείο για τη μείωση των κινδύνων ιδιωτικότητας. Σύμφωνα με τους Alpandinar, (2024), τα δεδομένα που δημιουργούνται γύρω από μια μεμονωμένη συσκευή ενδέχεται να μην είναι ευαίσθητα από μόνα τους, αλλά λόγω της διασυνδεδεμένης φύσης των δικτύων IoT που υπάρχουν σε έξυπνα σπίτια, μπορούν να αποκαλύψουν πληροφορίες όπως οι καταναλωτικές συνήθειες, τα πρότυπα συμπεριφοράς και άλλα δεδομένα που μπορεί να παρουσιάζουν σημαντικό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων δεδομένων. Η ανωνυμοποίηση πρέπει να εξετάζεται όσον αφορά τα νέα στοιχεία κάθε επεξεργασίας εντός εφαρμογών έξυπνου σπιτιού και έτσι να αναθεωρείται τακτικά προκειμένου να παραμείνει ένα αποτελεσματικό εργαλείο ασφάλειας.

2.2.7. Διαφάνεια και συναίνεση χρήστη

Η διαφάνεια στη συλλογή και επεξεργασία δεδομένων αποτελεί θεμελιώδη αρχή προστασίας ιδιωτικότητας. Οι Orlowski & Loh, (2025) επισημαίνουν ότι η συλλογή και επεξεργασία δεδομένων χρηστών σε περιβάλλοντα έξυπνων σπιτιών στερούνται επί του παρόντος διαφάνειας και ελέγχου. Σε πολλές περιπτώσεις, οι χρήστες δεν γνωρίζουν καν τη συλλογή δεδομένων συνολικά, ή τουλάχιστον όχι την έκτασή της. Ακόμη και όταν οι χρήστες είναι ενήμεροι γι' αυτά, οι επιλογές είναι πολύ

περιορισμένες. Συχνότερα, δεν έχουν άλλη επιλογή παρά να λάβουν αποφάσεις όλα ή τίποτα (να αγοράσουν ή να μην αγοράσουν τη συσκευή που αναφέρεται) αντιμέτωποι με προφανείς κινδύνους ιδιωτικότητας.

Η λήψη τεκμηριωμένης συγκατάθεσης είναι απαραίτητη για τη νόμιμη επεξεργασία προσωπικών δεδομένων. Οι κατασκευαστές πρέπει να ενημερώνουν σαφώς τους χρήστες σχετικά με τα δεδομένα που συλλέγονται και τον τρόπο με τον οποίο θα χρησιμοποιηθούν, διασφαλίζοντας ότι η συγκατάθεση λαμβάνεται με τρόπο που συμμορφώνεται με τις απαιτήσεις του GDPR (EpiSensor, 2024). Πριν ο χρήστης ξεκινήσει να χρησιμοποιεί ένα προϊόν IoT, ο προγραμματιστής παρέχει μια φόρμα συναίνεσης ιδιωτικότητας για τον χρήστη να συμπληρώσει. Ωστόσο, το περιεχόμενο της φόρμας συναίνεσης είναι συνήθως πολύ μεγάλο για τον χρήστη να διαβάσει, και ο χρήστης παραμελεί τις διατάξεις που σχετίζονται με τη χρήση ιδιωτικότητας, με αποτέλεσμα συχνά οι προσωπικές πληροφορίες να καταγράφονται στη βάση δεδομένων του προϊόντος χωρίς τη γνώση του χρήστη.

2.2.8. Ασφάλεια δικτύου και διαχωρισμός

Η ασφάλεια του οικιακού δικτύου Wi-Fi αποτελεί θεμελιώδη βήμα στην προστασία των συσκευών έξυπνου σπιτιού από εισβολές. Η ισχυρή κρυπτογράφηση, όπως το WPA3, είναι απαραίτητη για την αποφυγή υποκλοπής στις ασύρματες επικοινωνίες (Integrated Media Systems, 2024). Επιπλέον, η αλλαγή των προεπιλεγμένων ονομάτων δικτύου και κωδικών πρόσβασης καθιστά πιο δύσκολο για τους επιτιθέμενους να μαντέψουν τα διαπιστευτήρια. Η εφαρμογή ενός τείχους προστασίας λειτουργεί επίσης ως φραγμός, ελέγχοντας την εισερχόμενη και εξερχόμενη κίνηση δικτύου με βάση ένα εφαρμοσμένο σύνολο κανόνων, προστατεύοντας περαιτέρω τις συσκευές από πιθανές κυβερνοαπειλές.

Ο διαχωρισμός δικτύου (network segmentation) αποτελεί προηγμένη τεχνική ασφάλειας που απομονώνει τις συσκευές IoT από άλλες κρίσιμες συσκευές στο δίκτυο. Σύμφωνα με τους Olanrewaju et al. (2023), ο διαχωρισμός του δικτύου μπορεί να μειώσει τους κινδύνους που σχετίζονται με πιθανές παραβιάσεις ασφάλειας, περιορίζοντας την πλευρική κίνηση των επιτιθέμενων εντός του δικτύου. Η δημιουργία ξεχωριστών δικτύων ή VLANs για συσκευές IoT διασφαλίζει ότι ακόμη και αν μια έξυπνη συσκευή παραβιαστεί, ο επιτιθέμενος δεν μπορεί εύκολα να αποκτήσει

πρόσβαση σε άλλα ευαίσθητα συστήματα όπως υπολογιστές εργασίας ή συστήματα αποθήκευσης δεδομένων.

2.2.9. Ενημερώσεις firmware και διαχείριση ευπαθειών

Η τακτική ενημέρωση του firmware και του λογισμικού αποτελεί κρίσιμη πρακτική ασφάλειας για τη διατήρηση της ακεραιότητας των συσκευών IoT. Οι Magara et al. (2024) υπογραμμίζουν την πιεστική ανάγκη για μια ολοκληρωμένη και προληπτική προσέγγιση για την ασφάλεια των οικοσυστημάτων IoT, που περιλαμβάνει ισχυρή αυθεντικοποίηση, κρυπτογράφηση, συντήρηση firmware, ασφάλεια διεπαφής, διαχείριση ενημερώσεων, διαχείριση διαπιστευτηρίων, φυσική προστασία, εκπαίδευση χρηστών και διατήρηση ιδιωτικότητας. Οι συσκευές με ξεπερασμένο firmware μπορεί να περιέχουν μη επιδιορθωμένες τρύπες ασφάλειας που τις καθιστούν ευάλωτες σε γνωστές επιθέσεις.

Η διαχείριση ευπαθειών σε έξυπνα σπίτια απαιτεί συστηματική προσέγγιση. Οι 1NCE (2024) αναφέρουν ότι πολλές εταιρείες όπως η Mender μπορούν να βοηθήσουν τους παρόχους IoT να δημιουργήσουν ανθεκτικά οικοσυστήματα που προστατεύουν τους χρήστες, εξοικονομούν πόρους και ελέγχουν έργα IoT σε πραγματικό χρόνο. Η εφαρμογή των απαραίτητων τεχνικών διασφαλίσεων, οι κατασκευαστές μπορούν όχι μόνο να επιτύχουν συμμόρφωση αλλά και να επιδείξουν τη δέσμευσή τους στην οικοδόμηση εμπιστοσύνης με τους χρήστες τους στον διασυνδεδεμένο κόσμο. Οι ενημερώσεις Over-The-Air (OTA) επιτρέπουν στους κατασκευαστές να παρέχουν ενημερώσεις ασφάλειας από απόσταση, χωρίς να απαιτείται φυσική πρόσβαση στις συσκευές.

2.2.10. Εκπαίδευση και ευαισθητοποίηση χρηστών

Η εκπαίδευση των χρηστών αποτελεί κρίσιμο στοιχείο της στρατηγικής ασφάλειας για έξυπνα σπίτια. Πολλοί χρήστες δεν παρουσιάζονται με αρκετή γνώση των πρωτοκόλλων ασφάλειας για να χειριστούν αποτελεσματικά τις ανησυχίες ιδιωτικότητας· η έλλειψη ευαισθητοποίησης τους θέτει σε κίνδυνο για τον κίνδυνο παραβίασης των προσωπικών τους πληροφοριών (Albany et al., 2022). Η έρευνα προτείνει την ανάγκη για αποτελεσματικές στρατηγικές για τον μετριασμό των ζητημάτων ιδιωτικότητας και ασφάλειας που σχετίζονται με διασυνδεδεμένες έξυπνες

συσκευές σε σπίτια. Οι χρήστες πρέπει να είναι σε θέση να χρησιμοποιούν συσκευές IoT χωρίς να ανησυχούν για την ασφάλεια, την ιδιωτικότητα και την εμπιστευτικότητα των προσωπικών τους πληροφοριών.

Η ανάπτυξη προγραμμάτων εκπαίδευσης και ευαισθητοποίησης μπορεί να βελτιώσει σημαντικά το επίπεδο ασφάλειας των έξυπνων σπιτιών. Σύμφωνα με τους Vardakis et al., (2024), η σημασία της ευαισθητοποίησης και εκπαίδευσης των χρηστών στη διατήρηση της ασφάλειας των περιβαλλόντων έξυπνου σπιτιού είναι θεμελιώδης. Οι χρήστες που γνωρίζουν πώς μοιράζονται, ασφαλίζονται και προστατεύονται οι πληροφορίες τους είναι πιο πιθανό να βιώσουν ικανοποίηση και να λάβουν ενεργά μέτρα για την προστασία των συστημάτων τους. Η υποχρεωτική εκπαίδευση είναι απαραίτητη, αλλά η εκπαίδευση από εταιρείες outsourcing, που «ενισχύει την αντιπάθεια και θεωρείται μηχανική εργασία» αντί για πραγματική εμπειρία μάθησης, θα πρέπει να αποφεύγεται.

2.2.11. Νομοθετικό πλαίσιο και συμμόρφωση με το GDPR

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης έχει επηρεάσει καθοριστικά τον τρόπο με τον οποίο οι οργανισμοί χειρίζονται προσωπικά δεδομένα από συσκευές IoT. Ο GDPR εγκρίθηκε τον Απρίλιο του 2016 και άρχισε να ισχύει στις 25 Μαΐου 2018, αντικαθιστώντας την Οδηγία Προστασίας Δεδομένων που εκκινήθηκε από την Ευρωπαϊκή Ένωση το 1995 (Jhuang et al., 2023). Ο GDPR είναι ένας κανονισμός για την προστασία προσωπικών δεδομένων και της ιδιωτικότητας όλων των πολιτών της ΕΕ στα νομικά πλαίσια της ΕΕ, και εφαρμόζεται σε χώρες που ανήκουν στην ΕΕ και σε όλες τις επιχειρήσεις που έχουν επιχειρηματικές συναλλαγές με χώρες της ΕΕ, ανεξάρτητα από την τοποθεσία τους.

Το GDPR επιβάλλει ότι οι οργανισμοί πρέπει να ασφαλίσουν τα προσωπικά δεδομένα που συλλέγονται από συσκευές IoT, να υλοποιήσουν την ιδιωτικότητα με σχεδιασμό (privacy by design) και να διασφαλίσουν τα δικαιώματα των υποκειμένων δεδομένων (1NCE, 2024). Έχουν επιφέρει αυστηρές ποινές για την έλλειψη συμμόρφωσης ως μοντέλο πολλών στόχων προστασίας παγκοσμίως. Οι βασικές απαιτήσεις του GDPR που επηρεάζουν το IoT περιλαμβάνουν την ελαχιστοποίηση δεδομένων (συλλογή μόνο των απαραίτητων δεδομένων για τον προβλεπόμενο σκοπό), τη συγκατάθεση (λήψη ρητής συγκατάθεσης από τους χρήστες πριν από τη συλλογή και επεξεργασία των

δεδομένων τους), και το δικαίωμα στη λήθη (επιτρέποντας στους χρήστες να ζητήσουν τη διαγραφή των προσωπικών τους δεδομένων).

2.2.12. Πρότυπα ασφάλειας IoT και πιστοποιήσεις

Τα διεθνή πρότυπα ασφάλειας παίζουν κρίσιμο ρόλο στη διασφάλιση της ασφάλειας των συσκευών έξυπνου σπιτιού. Το ETSI EN 303 645 ή το IEC 62443 μπορούν ήδη να χρησιμοποιηθούν για την επίδειξη συμμόρφωσης προϊόντων IoT έναντι των ελάχιστων απαιτήσεων ασφάλειας της ΕΕ (Bureau Veritas, 2024). Η Ευρωπαϊκή Επιτροπή έχει επιβάλει ελάχιστες απαιτήσεις για την ασφάλεια των προϊόντων IoT, γνωστών ως έξυπνες συσκευές, ξεκινώντας το 2024. Εάν δεν πληρούν αυτά τα πρότυπα, το προϊόν θα απαγορευτεί από την αγορά της ΕΕ. Οι ελάχιστες βασικές απαιτήσεις ασφάλειας υπάρχουν για να προστατεύσουν τόσο τις επιχειρήσεις όσο και τους καταναλωτές από πιθανές κυβερνοεπιθέσεις.

Η Ευρωπαϊκή Επιτροπή Προστασίας Δεδομένων (EDPB) παρέχει καθοδήγηση για την εφαρμογή των αρχών προστασίας δεδομένων στο πλαίσιο του IoT. Οι ειδικοί υπογράμμισαν την έλλειψη επαρκών κωδίκων συμπεριφοράς ειδικά για τον τομέα (για τον τομέα IoT), οδηγιών από τις Αρχές Προστασίας Δεδομένων που αφορούν ευάλωτα άτομα γενικά και συμβουλών σχετικά με τον τρόπο συμπερίληψης της ευπάθειας στις Εκτιμήσεις Αντικτύπου Προστασίας Δεδομένων (DPIAs) (Piasecki, 2023). Η ανάπτυξη τομεακών κωδίκων συμπεριφοράς και προτύπων μπορεί να βοηθήσει τις εταιρείες να επιδείξουν συμμόρφωση με το GDPR και τους ρυθμιστές να διασφαλίσουν την εφαρμογή των διατάξεων προστασίας δεδομένων.

2.2.13. Εκτίμηση αντικτύπου προστασίας δεδομένων (DPIA)

Η διενέργεια Εκτιμήσεων Αντικτύπου Προστασίας Δεδομένων (DPIAs) αποτελεί απαραίτητη πρακτική για έργα IoT. Οι DPIAs αξιολογούν τον πιθανό αντίκτυπο των έργων IoT στην ιδιωτικότητα δεδομένων και εφαρμόζουν μέτρα για τον μετριασμό των κινδύνων (EpiSensor, 2024). Οι DPIAs βοηθούν στον εντοπισμό ευπαθειών και διασφαλίζουν τη συμμόρφωση με το GDPR και άλλους κανονισμούς. Όταν πρόκειται για παιδιά που ζουν σε έξυπνα σπίτια, η συμμόρφωση με το GDPR απαιτεί την επιβολή τεχνικών και οργανωτικών μέτρων σχετικά με συγκεκριμένη επεξεργασία δεδομένων. Αυτό συνεπάγεται εννέα κριτήρια που έχουν υιοθετηθεί, προκειμένου να καθοριστεί η

διενέργεια DPIA και η δημιουργία συγκεκριμένων καταλόγων από τα κράτη μέλη σε εθνικό επίπεδο (Mercz, 2024).

Η συστηματική αξιολόγηση κινδύνων μέσω DPIA επιτρέπει στους οργανισμούς να προσδιορίσουν πιθανές απειλές και να αναπτύξουν κατάλληλες στρατηγικές μετριασμού. Οι Abu-Tair et al. (2024) προτείνουν ότι η προτεινόμενη λύση μπορεί να εφαρμοστεί σε οικιακά περιβάλλοντα όπου μια κεντρικοποιημένη πηγή αλήθειας, όπως ένα σημείο πρόσβασης στο Διαδίκτυο BT HomeHub, μπορεί να διασφαλίσει ότι όλες οι συσκευές IoT που προσπαθούν να συνδεθούν μέσω αυτού συμμορφώνονται με νομικές υποχρεώσεις και κανονισμούς όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR). Αυτή η προσέγγιση μπορεί να αυτοματοποιήσει τη διαδικασία επαλήθευσης συμμόρφωσης και να διασφαλίσει ότι μόνο ασφαλείς συσκευές επιτρέπεται να συνδεθούν στο δίκτυο του έξυπνου σπιτιού.

2.2.14. Τεχνολογίες blockchain και distributed ledger

Οι τεχνολογίες blockchain προσφέρουν υποσχόμενες λύσεις για την ενίσχυση της ασφάλειας και της ιδιωτικότητας στα έξυπνα σπίτια. Ο μηχανισμός συναίνεσης είναι μια τεχνολογία μνήμης blockchain, η οποία είναι μία από τις πιο βασικές τεχνολογίες (Jhuang et al., 2023). Είναι ένας μηχανισμός που χρησιμοποιείται για να διασφαλιστεί ότι οι συμμετέχοντες φτάνουν σε συναίνεση και επιτυγχάνουν εμπιστοσύνη μεταξύ των μπλοκ μέσω αποκεντρωμένων αλγορίθμων συναίνεσης. Επί του παρόντος, ο μηχανισμός συναίνεσης εφαρμόζεται στον τομέα του κρυπτονομίσματος, παρέχοντας δικαιοσύνη, αποτελεσματικότητα και συνέπεια στις συναλλαγές.

Η ενσωμάτωση της τεχνολογίας blockchain για την ενίσχυση της ασφάλειας των συσκευών IoT αποτελεί αυξανόμενη τάση. Οι Magara et al. (2024) αναφέρουν ότι οι πρόσφατες εξελίξεις στη διαλειτουργικότητα IoT περιλαμβάνουν την πρόταση τυποποιημένων πρωτοκόλλων, την τήρηση διεθνών προτύπων, την πλήρωση απαιτήσεων ασφάλειας και την επεκτασιμότητα. Επιπλέον, υπάρχει μια αυξανόμενη τάση προς την ενσωμάτωση της τεχνολογίας blockchain για την ενίσχυση της ασφάλειας των συσκευών IoT. Το blockchain μπορεί να παρέχει αμετάβλητα αρχεία συναλλαγών, αποκεντρωμένο έλεγχο και ενισχυμένη διαφάνεια, καθιστώντας το ιδανικό για την ασφάλιση των επικοινωνιών μεταξύ συσκευών IoT σε έξυπνα σπίτια.

2.2.15. Τεχνητή νοημοσύνη και μηχανική μάθηση για ασφάλεια

Η εφαρμογή αλγορίθμων τεχνητής νοημοσύνης και μηχανικής μάθησης προσφέρει προηγμένες δυνατότητες για την ανίχνευση και πρόληψη απειλών. Οι Vardakis et al., (2024) προτείνουν τη χρήση αλγορίθμων Τεχνητής Νοημοσύνης (AI) και Μηχανικής Μάθησης (ML) για την ανίχνευση ασυνήθιστης συμπεριφοράς που μπορεί να υποδεικνύει παραβίαση ασφάλειας. Αυτές οι τεχνολογίες μπορούν να αναλύσουν μεγάλους όγκους δεδομένων από συσκευές έξυπνου σπιτιού, να εντοπίσουν ανωμαλίες και να αντιδράσουν σε απειλές σε πραγματικό χρόνο. Οι Rahman et al. (2024) παρέχουν μια ολοκληρωμένη ανασκόπηση των προσεγγίσεων μηχανικής μάθησης για την ανίχνευση ανωμαλιών σε έξυπνα σπίτια, επιδεικνύοντας πειραματική ανάλυση και μελλοντικές κατευθύνσεις.

Ωστόσο, με την εμφάνιση της τεχνητής νοημοσύνης και τα οφέλη που προσφέρει, είναι ευάλωτη σε πολυάριθμες προκλήσεις. Οι τρέχουσες προκλήσεις ασφάλειας AI περιλαμβάνουν επιθέσεις εναντίον μοντέλων (adversarial attacks), ανησυχίες ιδιωτικότητας, μεροληψία, ευπάθειες ασφάλειας μοντέλων, ζητήματα αξιοπιστίας, κενά εξηγησιμότητας, δηλητηρίαση δεδομένων και προκλήσεις επεκτασιμότητας (Magara et al., 2024). Απαιτούνται διεπιστημονικές προσπάθειες για την ενίσχυση της ευρωστίας, της διαφάνειας και της κανονιστικής συμμόρφωσης, ενώ παράλληλα μετριάζονται οι κίνδυνοι για την ιδιωτικότητα, τη δικαιοσύνη και την πνευματική ιδιοκτησία.

2.2.16. Προοπτικές και μελλοντικές κατευθύνσεις

Η μελλοντική έρευνα στην ασφάλεια και ιδιωτικότητα έξυπνων σπιτιών πρέπει να επικεντρωθεί σε διάφορους τομείς. Οι Vardakis et al., (2024) προτείνουν μελλοντικές ερευνητικές κατευθύνσεις και συστάσεις για την ενίσχυση της ασφάλειας έξυπνου σπιτιού με το IoT, συμπεριλαμβανομένης της ανάπτυξης ισχυρών βέλτιστων πρακτικών και προτύπων ασφάλειας, βελτιωμένων μεθόδων αυθεντικοποίησης συσκευών και πιο αποτελεσματικών τεχνικών ανίχνευσης εισβολών. Αντιμετωπίζοντας αυτές τις προκλήσεις, η δυνατότητα των έξυπνων σπιτιών με δυνατότητα IoT να ενισχύσουν την ευκολία και την αποτελεσματικότητα διασφαλίζοντας παράλληλα την ιδιωτικότητα, την ασφάλεια και την κυβερνοανθεκτικότητα μπορεί να πραγματοποιηθεί.

Η ανάγκη για επεκτάσιμες εναλλακτικές λύσεις στην παραδοσιακή άμυνα περιμέτρου, καθώς τα δίκτυα IoT απαιτούν πιο προσαρμοστικές διαδικασίες ασφάλειας, αποτελεί κρίσιμη προτεραιότητα (Magara et al., 2024). Προτείνονται νέοι τρόποι διαχείρισης της ασφάλειας εντός των αναπτυγμένων δικτύων IoT, αναγνωρίζοντας τα μοναδικά προβλήματα της διασφάλισης μεγάλου αριθμού συνδεδεμένων συσκευών. Προτείνονται νέες πολιτικές ασφάλειας που παρέχουν την απαραίτητη γενικότητα για τη ρύθμιση συσκευών και δικτύων IoT σε ένα ευρύ φάσμα περιπτώσεων χρήσης, αναγνωρίζοντας την ανάγκη για ευελιξία στην ασφάλεια IoT. Η αποτελεσματική αντιμετώπιση αυτών των προκλήσεων απαιτεί την ανάπτυξη επεκτάσιμων λύσεων, καινοτόμων στρατηγικών διαχείρισης και προσαρμόσιμων πλαισίων πολιτικής.

3. Βιβλιογραφική ανασκόπηση

Η ραγδαία εξάπλωση των έξυπνων σπιτιών και των συσκευών IoT έχει οδηγήσει σε μια αντίστοιχη έκρηξη ερευνητικού ενδιαφέροντος γύρω από ζητήματα ασφάλειας και προστασίας της ιδιωτικότητας. Πλέον δεν πρόκειται απλώς για μεμονωμένες «έξυπνες» συσκευές, αλλά για ολόκληρα οικοσυστήματα δικτυωμένων αισθητήρων, καμερών, φωνητικών βοηθών, κλειδαριών και ιατρικών συσκευών, τα οποία συλλέγουν, επεξεργάζονται και διακινούν ευαίσθητα δεδομένα των ενοίκων. Σύμφωνα με τον Mocrii και τους συνεργάτες του, τα έξυπνα σπίτια αποτελούν χαρακτηριστικό παράδειγμα σύγκλισης υπολογιστικού νέφους, κινητών συσκευών και δικτυωμένων αισθητήρων, δημιουργώντας ένα περιβάλλον όπου η ασφάλεια δεν μπορεί να αντιμετωπιστεί αποσπασματικά, αλλά απαιτεί μια ολιστική, πολυεπίπεδη προσέγγιση (Mocrii et al., 2018).

Παράλληλα, μελέτες αγοράς που παραθέτουν οι Bugeja et al. δείχνουν ότι η παγκόσμια αγορά smart home εκτιμήθηκε περίπου στα 9,8 δισεκατομμύρια δολάρια το 2015, με πρόβλεψη να φτάσει τα 43 δισεκατομμύρια δολάρια έως το 2020, ενώ νεότερες εκτιμήσεις ανέβαζαν την αξία της αγοράς στα 53,45 δισεκατομμύρια δολάρια το 2022. Παράλληλα, η μελέτη των Zeng et al. αναφέρει ότι ήδη από το 2017 υπήρχαν εκατοντάδες εκατομμύρια έξυπνες συσκευές εγκατεστημένες σε περισσότερα από 40 εκατομμύρια σπίτια μόνο στις ΗΠΑ, με τις προβλέψεις να κάνουν λόγο για διπλασιασμό αυτού του αριθμού μέσα σε λίγα χρόνια. (Zeng et al., 2017). Η κλίμακα αυτή υπογραμμίζει ότι ακόμη και «σπάνια» τρωτά σημεία μπορούν να μετατραπούν σε μαζικό πρόβλημα ασφάλειας και ιδιωτικότητας.

Εντός αυτού του πλαισίου, η βιβλιογραφία μπορεί να ομαδοποιηθεί σε τρεις μεγάλες κατηγορίες, οι οποίες αντιστοιχούν και στις υποενότητες του παρόντος κεφαλαίου: μελέτες που αναλύουν συγκεκριμένες επιθέσεις και σενάρια απειλών σε έξυπνα σπίτια, εργασίες που προτείνουν σύγχρονες τεχνικές και αρχιτεκτονικές για την ενίσχυση της ασφάλειας IoT, και, τέλος, ερευνητικές προσεγγίσεις που εστιάζουν στην ιδιωτικότητα και τη συμπεριφορά των χρηστών. Στη συνέχεια παρουσιάζονται αναλυτικά οι τρεις αυτές ερευνητικές κατευθύνσεις, με έμφαση τόσο στα ποιοτικά ευρήματα όσο και στα ποσοτικά δεδομένα που αναδεικνύουν το μέγεθος και τη φύση του προβλήματος.

3.1 Παρουσίαση ερευνητικών εργασιών για επιθέσεις σε smart homes

Η βιβλιογραφία γύρω από τις επιθέσεις σε έξυπνα σπίτια μπορεί να χωριστεί, σε γενικές γραμμές, σε δύο τύπους εργασιών: πειραματικές μελέτες που επιδεικνύουν συγκεκριμένες τεχνικές επιθέσεων σε συσκευές ή πλατφόρμες smart home και συστηματικές ανασκοπήσεις που χαρτογραφούν το τοπίο των απειλών.

Οι Bugeja et al. ήδη από το 2016 ανέδειξαν, σε μια ευρέως αναφερόμενη μελέτη, το μέγεθος της έκθεσης που προκύπτει από ελλιπή ρυθμίσεις ασφαλείας και αδύναμους μηχανισμούς αυθεντικοποίησης. Αναλύοντας τη διαθεσιμότητα δικτυωμένων καμερών επιτήρησης, εντόπισαν πάνω από 73.000 IP κάμερες που μετέδιδαν δημόσια βίντεο στο διαδίκτυο, πολλές φορές εν αγνοία των ιδιοκτητών τους (Bugeja et al., 2016).

Το συγκεκριμένο εύρημα είναι ενδεικτικό της ευρείας επιφάνειας επίθεσης που δημιουργείται όταν συσκευές με αδύναμα προεπιλεγμένα διαπιστευτήρια ή λανθασμένη διαμόρφωση εκτίθενται απευθείας στο διαδίκτυο. Αντίστοιχα, οι Geneiatakis et al. πραγματοποίησαν εις βάθος ανάλυση απειλών σε ένα τυπικό IoT–βασισμένο έξυπνο σπίτι, περιγράφοντας ρεαλιστικά σενάρια επίθεσης σε «κρίσιμες» συσκευές, όπως έξυπνες κλειδαριές, κάμερες και θερμοστάτες (Geneiatakis et al., 2017).

Η ανάλυσή τους δείχνει πώς, μέσω συνδυασμού επιθέσεων σε επίπεδο δικτύου (π.χ. ARP spoofing), εφαρμογών και cloud υπηρεσιών, ένας επιτιθέμενος μπορεί να αποκτήσει πλήρη έλεγχο σε λειτουργίες όπως το κλείδωμα/ξεκλείδωμα θυρών ή η παρακολούθηση χώρων, με άμεσο κίνδυνο για τη φυσική ασφάλεια των ενοίκων.

Μια άλλη σημαντική κατηγορία επιθέσεων αφορά στη χρήση των συσκευών smart home ως «όπλο» για επιθέσεις ευρύτερης κλίμακας στο διαδίκτυο. Η επίθεση Mirai, στην οποία αναφέρονται οι Zeng et al., έδειξε ότι ένας μεγάλος αριθμός ευάλωτων IoT συσκευών μπορεί να στρατολογηθεί σε botnet και να χρησιμοποιηθεί για επιθέσεις DDoS μεγάλης κλίμακας, επηρεάζοντας εκατομμύρια χρήστες (Zeng et al., 2017). Η ύπαρξη εκατομμυρίων συσκευών με κοινά προεπιλεγμένα passwords δημιουργεί, επομένως, όχι μόνο κίνδυνο για το μεμονωμένο σπίτι, αλλά και για την ευρύτερη υποδομή του διαδικτύου.

Εστιάζοντας στις επιθέσεις σε επίπεδο εφαρμογής και πλατφόρμας, αρκετές εργασίες έχουν δείξει ότι οι κανόνες αυτοματοποίησης και οι εφαρμογές τρίτων κατασκευαστών μπορούν να αποτελέσουν σημαντικό φορέα κινδύνου. Η ανάλυση των Fernandes et al. (που συζητείται, μεταξύ άλλων, από τους Zeng και Roesner) αποκαλύπτει ότι πολλές πλατφόρμες τύπου SmartThings επιτρέπουν σε εφαρμογές να ζητούν υπερβολικά δικαιώματα, οδηγώντας σε υπερεξουσιοδότηση και δυνατότητα εκτέλεσης ενεργειών που ο χρήστης δεν αντιλαμβάνεται ή δεν έχει συνειδητά επιτρέψει (Zeng & Roesner, 2019).

Στο ίδιο πνεύμα, ο Bugeja και οι συνεργάτες του αναλύουν «σημασιολογικές» επιθέσεις άρνησης υπηρεσίας (semantic DoS), όπου ο επιτιθέμενος δεν επιδιώκει απλώς να καταρρίψει το δίκτυο, αλλά να εκμεταλλευτεί τους κανόνες αυτοματοποίησης, δημιουργώντας αλυσιδωτές, ενοχλητικές ή επικίνδυνες ενέργειες μέσα στο σπίτι (για παράδειγμα, επαναλαμβανόμενο άνοιγμα/κλείσιμο φώτων ή κλειδαριών) (Bugeja et al., 2021).

Σε επίπεδο συστηματικών ανασκοπήσεων, η εργασία των Abid et al. επιχειρεί μια ταξινόμηση των επιθέσεων σε έξυπνα σπίτια ανά στρώμα (αντίληψης, δικτύου, εφαρμογής) και τύπο απειλής, καταδεικνύοντας ότι η πλειονότητα των δημοσιευμένων επιθέσεων στοχεύει το επίπεδο εφαρμογής και το ασύρματο δίκτυο, ενώ λιγότερες – αλλά ιδιαίτερα κρίσιμες– εργασίες αφορούν επιθέσεις στην ίδια τη φυσική υποδομή και στους αισθητήρες (Dhanraj et al., 2024). Επιπλέον, οι συγγραφείς συνδέουν το αυξανόμενο ενδιαφέρον για τέτοιες επιθέσεις με την εκρηκτική αύξηση των IoT συσκευών, η οποία σε άλλες πηγές εκτιμάται σε δεκάδες δισεκατομμύρια συσκευές τα επόμενα χρόνια.

Η μελέτη των Khan et al. υιοθετεί μια λίγο διαφορετική οπτική, καθώς εξετάζει συστηματικά τους κινδύνους ασφάλειας και ασφάλειας ζωής (safety and security risks) σε έξυπνα κτίρια και σπίτια, με έμφαση σε καταστάσεις έκτακτης ανάγκης. Μέσω Systematic Literature Review, οι συγγραφείς κατέληξαν σε ένα τελικό σύνολο 99 σχετικών ερευνητικών εργασιών, δημοσιευμένων μεταξύ 2016 και 2020, που εξετάζουν τόσο την ασφάλεια από κυβερνοεπιθέσεις όσο και την προστασία των ενοίκων σε συνθήκες πυρκαγιάς, σεισμού ή άλλων κινδύνων (Khan et al., 2021). Η ποσοτική αυτή επισκόπηση δείχνει ότι το ερευνητικό ενδιαφέρον για τους κινδύνους

στα smart homes αυξήθηκε σημαντικά μετά το 2016, σε παράλληλη πορεία με την αυξανόμενη εμπορική υιοθέτηση.

Σε επίπεδο λεπτομερούς risk assessment, η εργασία των Jacobsson, Boldt και Carlsson πραγματοποιεί μια αναλυτική ανάλυση κινδύνου σε ένα συγκεκριμένο σύστημα οικιακού αυτοματισμού. Οι συγγραφείς εντοπίζουν 32 πιθανούς κινδύνους ασφάλειας, από τους οποίους 9 χαρακτηρίζονται ως χαμηλού, 4 ως υψηλού και οι υπόλοιποι ως μεσαίου επιπέδου κινδύνου, υποδεικνύοντας ότι η πλειοψηφία των απειλών σε ένα πραγματικό σύστημα δεν είναι ακραίες, αλλά αθροίζονται για να δημιουργήσουν μια ιδιαίτερα εκτεταμένη επιφάνεια ευπάθειας (Bugeja et al., 2021). Το ποσοτικό αυτό αποτέλεσμα υπογραμμίζει τη σημασία μεθοδολογιών risk assessment που δεν επικεντρώνονται μόνο στις «κραυγαλέες» απειλές, αλλά αξιολογούν συστηματικά και τις πιο «ήπιες» παραβιάσεις ή αδυναμίες.

Τέλος, η εργασία των Shouran et al. προσεγγίζει τις επιθέσεις στα smart homes μέσα από το κλασικό τρίπτυχο εμπιστευτικότητα – ακεραιότητα – διαθεσιμότητα, προτείνοντας μια ταξινόμηση των απειλών σε τέσσερα επίπεδα σοβαρότητας: χαμηλή, μέση, υψηλή και εξαιρετικά υψηλή (Shouran et al., 2019). Η κατηγοριοποίηση αυτή είναι χρήσιμη για την προτεραιοποίηση των μέτρων άμυνας, καθώς δείχνει ότι ορισμένες επιθέσεις (π.χ. διαρροή κάποιων μη ευαίσθητων δεδομένων) μπορεί να είναι διαχειρίσιμες, ενώ άλλες (όπως η μη εξουσιοδοτημένη πρόσβαση σε κλειδαριές ή ιατρικές συσκευές) πρέπει να αντιμετωπίζονται ως εξαιρετικά υψηλού κινδύνου λόγω των πιθανών επιπτώσεων στη σωματική ακεραιότητα των χρηστών.

Η βιβλιογραφία για τις επιθέσεις στα smart homes αποτυπώνει ένα ιδιαίτερα σύνθετο τοπίο απειλών, όπου η τεχνολογική πολυπλοκότητα συνδυάζεται με την άμεση σύνδεση του κυβερνοχώρου με τον φυσικό χώρο κατοικίας, καθιστώντας την ασφάλεια κρίσιμο ζήτημα τόσο από τεχνική όσο και από κοινωνική σκοπιά.

3.1.1. Αδυναμίες σε επίπεδο συσκευών (sensors, cameras, smart locks)

Η ασφάλεια των συσκευών σε ένα έξυπνο σπίτι αποτελεί θεμελιώδη παράγοντα για τη συνολική ανθεκτικότητα του οικοσυστήματος. Οι συσκευές πρώτης γραμμής –όπως αισθητήρες (sensors), κάμερες και smart locks– αποτελούν συχνά την πιο εκτεθειμένη και ευάλωτη κατηγορία εξοπλισμού, λόγω περιορισμένων υπολογιστικών πόρων,

ανεπαρκών μηχανισμών ελέγχου πρόσβασης και ελλιπούς σχεδιασμού ως προς την ασφάλεια. Η βιβλιογραφία υποδεικνύει ότι οι αδυναμίες αυτές εντοπίζονται τόσο σε επίπεδο υλικού (hardware) όσο και λογισμικού (firmware και εφαρμογές), καθιστώντας τις συσκευές στόχο επιθέσεων που μπορούν να οδηγήσουν σε παραβίαση ιδιωτικότητας, μη εξουσιοδοτημένη πρόσβαση και αλλοίωση δεδομένων.

Οι Chhetri και Motti (2020) επισημαίνουν ότι η μεγάλη ποικιλία συσκευών και προτύπων στην υλοποίηση έξυπνων οικιακών συστημάτων δημιουργεί ένα ανομοιογενές περιβάλλον, όπου οι μη ασφαλείς προεπιλεγμένες ρυθμίσεις, η έλλειψη τακτικών ενημερώσεων λογισμικού και η ελάχιστη κρυπτογράφηση αποτελούν συχνά σημεία εισόδου για επιτιθέμενους. Ένα από τα βασικά προβλήματα που αναγνωρίζεται στις έρευνες αφορά στην αδυναμία των κατασκευαστών να ενσωματώσουν μηχανισμούς ασφαλείας που να συμβαδίζουν με το χαμηλό κόστος παραγωγής. Το αποτέλεσμα είναι συσκευές που διαθέτουν είτε καθόλου είτε ανεπαρκείς μηχανισμούς θωράκισης, επιτρέποντας σε κακόβουλους χρήστες να εκμεταλλευτούν ανοιχτές θύρες, μη ασφαλή firmware ή ασθενείς μηχανισμούς αυθεντικοποίησης.

Στο πεδίο των έξυπνων καμερών, η βιβλιογραφία αναδεικνύει σημαντικές αδυναμίες, ιδιαίτερα όσον αφορά στην ανεπαρκή προστασία των διαύλων μετάδοσης δεδομένων και των firmware images. Οι Alharbi και Aspinall (2018) εντοπίζουν πολλαπλά σημεία ευπάθειας σε smart cameras, όπως αδύναμα credentials, έλλειψη ασφαλούς κρυπτογράφησης στις ροές βίντεο και δυνατότητα παράκαμψης μηχανισμών authentication. Οι ερευνητές υπογραμμίζουν ότι πολλές κάμερες IoT επιτρέπουν την πρόσβαση μέσω web interfaces που δεν διαθέτουν σύγχρονες πολιτικές ασφαλείας, καθιστώντας εφικτές επιθέσεις brute-force ή credential stuffing. Παράλληλα, στη μελέτη των Bhardwaj et al. (2023), η ανάλυση firmware έξυπνων καμερών αποκάλυψε την ύπαρξη σκληροκωδικοποιημένων κωδικών, μη ενημερωμένων βιβλιοθηκών λογισμικού και μη ασφαλών υπηρεσιών debugging, τα οποία επιτρέπουν σε έναν επιτιθέμενο να αποκτήσει πλήρη έλεγχο της συσκευής.

Οι Sivaraman et al. (2018) υπογραμμίζουν ότι η δημοφιλία των έξυπνων καμερών όχι μόνο επεκτείνει την επιφάνεια προσβολής, αλλά αυξάνει και τον κίνδυνο παραβίασης της ιδιωτικότητας, καθώς μια παραβιασμένη κάμερα αποτελεί μέσο συνεχούς παρακολούθησης του περιβάλλοντος. Η ανάλυσή τους δείχνει ότι ακόμη και όταν τα

δεδομένα είναι κρυπτογραφημένα, οι επιτιθέμενοι μπορούν να εξάγουν πληροφορίες από side-channel χαρακτηριστικά της κίνησης δικτύου, όπως συχνότητα και μέγεθος πακέτων (Apthorpe et al., 2017). Αυτό αποδεικνύει ότι οι απειλές σε επίπεδο συσκευών δεν περιορίζονται μόνο στη δυνατότητα πλήρους παραβίασης αλλά περιλαμβάνουν και πιο λεπτές μορφές «παρατήρησης», οι οποίες παραβιάζουν την ιδιωτικότητα χωρίς να απαιτείται άμεση πρόσβαση στο ίδιο το υλικό.

Αντίστοιχα, τα έξυπνα κλειδαριές (smart locks) αποτελούν κρίσιμες συσκευές, καθώς ο έλεγχος πρόσβασης στον φυσικό χώρο εξαρτάται άμεσα από την ακεραιότητά τους. Οι Caballero-Gil et al. (2024) εντόπισαν σημαντικές αδυναμίες στα πρωτόκολλα αυθεντικοποίησης των smart locks, περιλαμβανομένων ασθενών κλειδιών κρυπτογράφησης και ανεπαρκών μηχανισμών προστασίας έναντι replay attacks. Επιπλέον, αρκετές συσκευές βρέθηκε ότι επιτρέπουν τη διαχείριση πρόσβασης μέσω μη ασφαλών Bluetooth Low Energy διαύλων, με αποτέλεσμα ένας επιτιθέμενος να μπορεί να αναπαράγει ή να υποκλέψει πακέτα επικοινωνίας. Οι Wolniak (2024) τονίζουν ότι πολλά smart locks προωθούνται στην αγορά ως «υψηλής ασφάλειας», χωρίς ωστόσο να συνοδεύονται από τυποποιημένες μεθόδους αξιολόγησης κυβερνοασφάλειας, γεγονός που σημαίνει ότι οι χρήστες συχνά υιοθετούν συσκευές των οποίων η αντοχή σε επιθέσεις δεν έχει επαρκώς τεκμηριωθεί.

Στον τομέα των αισθητήρων (sensors), οι αδυναμίες δεν περιορίζονται μόνο στο λογισμικό αλλά συχνά σχετίζονται με την ίδια τη φυσική τους κατασκευή. Αισθητήρες κίνησης, θερμοκρασίας ή φωτός μπορεί να υποστούν spoofing μέσω τεχνητών σημάτων, όπως υπεριώδης ακτινοβολία ή μεταβολές θερμοκρασίας που προσομοιώνουν πραγματική δραστηριότητα. Οι Davis et al. (2020) επισημαίνουν ότι πολλές IoT συσκευές βασίζονται σε αδύναμους μηχανισμούς ταυτοποίησης δεδομένων, γεγονός που επιτρέπει σε εισβολείς να εισάγουν ψευδή δεδομένα (data injection attacks) τα οποία παραπλανούν το σύστημα αυτοματισμού ενός έξυπνου σπιτιού.

Πέρα από τις επιθέσεις spoofing, η βιβλιογραφία αναδεικνύει και ζητήματα που σχετίζονται με την ελλιπή απομόνωση των λειτουργιών των αισθητήρων. Οι Park et al. (2019) δείχνουν ότι μια παραβιασμένη συσκευή μπορεί να λειτουργήσει ως pivot, επιτρέποντας στον εισβολέα να κινηθεί πλευρικά στο δίκτυο και να αποκτήσει

πρόσβαση σε πιο κρίσιμες συσκευές. Σε ορισμένες περιπτώσεις, οι επιτιθέμενοι εκμεταλλεύονται παραλείψεις στον τρόπο με τον οποίο γίνεται η αποθήκευση δεδομένων τοπικά, αποκτώντας πρόσβαση σε ιστορικά δεδομένα που αποκαλύπτουν συνήθειες και μοτίβα κίνησης των χρηστών.

Οι μελέτες δείχνουν επίσης ότι ένα σημαντικό ποσοστό των αδυναμιών των συσκευών προκύπτει από την έλλειψη συστηματικών ενημερώσεων firmware. Πολλοί κατασκευαστές είτε δεν διαθέτουν οργανωμένο μηχανισμό OTA (over-the-air) updates είτε διακόπτουν την υποστήριξη συσκευών πρόωρα. Αυτό οδηγεί σε συσκευές που παραμένουν εκτεθειμένες σε γνωστές ευπάθειες για μεγάλα χρονικά διαστήματα. Οι Jose και Malekian (2017) αναφέρουν ότι η ενσωμάτωση «λογικής» στα συστήματα αισθητήρων και αυτοματισμού, χωρίς παράλληλη ενίσχυση των μηχανισμών ασφαλείας, δημιουργεί επιπλέον κινδύνους, καθώς οι επιθέσεις μπορούν να επηρεάσουν πολλαπλές λειτουργίες του συστήματος, προκαλώντας αλυσιδωτές επιπτώσεις.

Τέλος, η ανάλυση των παραπάνω ευρημάτων καταδεικνύει ότι οι επιθέσεις που στοχεύουν συσκευές smart home δεν χρειάζονται πάντοτε υψηλή τεχνική εξειδίκευση. Πολλές ευπάθειες είναι αποτέλεσμα κακών πρακτικών σχεδιασμού, όπως η χρήση κοινών default passwords, η μη κρυπτογραφημένη μετάδοση δεδομένων ή η έλλειψη μηχανισμών logging. Συνεπώς, οι αδυναμίες σε επίπεδο συσκευών αποτελούν όχι μόνο τεχνικό αλλά και οργανωτικό ζήτημα, όπου ο ρόλος των κατασκευαστών, των προτύπων βιομηχανίας και της ενημέρωσης των χρηστών είναι καθοριστικός.

Η βιβλιογραφία αποδεικνύει ότι οι συσκευές των έξυπνων σπιτιών βρίσκονται στο επίκεντρο της επιφάνειας επίθεσης, καθώς συνδυάζουν περιορισμένη υπολογιστική ισχύ, ετερογένεια τεχνολογιών και συχνές ελλείψεις σε πρακτικές ασφαλούς σχεδιασμού. Οι επιπτώσεις από την εκμετάλλευση αυτών των αδυναμιών είναι ιδιαίτερα σοβαρές, επηρεάζοντας τόσο την ιδιωτικότητα όσο και την ασφάλεια του φυσικού χώρου. Αυτό καθιστά αναγκαία την περαιτέρω έρευνα, την ανάπτυξη ασφαλέστερων προτύπων και την ενίσχυση των μηχανισμών προστασίας σε όλα τα στάδια του κύκλου ζωής των έξυπνων συσκευών.

3.1.2. Επιθέσεις σε πρωτόκολλα επικοινωνίας (Wi-Fi, Zigbee, Z-Wave, Bluetooth)

Τα πρωτόκολλα επικοινωνίας αποτελούν τη θεμελιώδη υποδομή μέσω της οποίας λειτουργεί το οικοσύστημα των έξυπνων σπιτιών. Η δυνατότητα των συσκευών IoT να ανταλλάσσουν δεδομένα σε πραγματικό χρόνο, να συγχρονίζονται και να λειτουργούν σε αρμονία εξαρτάται άμεσα από την ασφάλεια των διαύλων επικοινωνίας που χρησιμοποιούν. Ωστόσο, η βιβλιογραφία αποκαλύπτει ότι τα πρωτόκολλα που κυριαρχούν στα έξυπνα σπίτια –Wi-Fi, Zigbee, Z-Wave και Bluetooth– εμφανίζουν σημαντικές αδυναμίες τόσο σε επίπεδο σχεδιασμού όσο και σε επίπεδο υλοποίησης, καθιστώντας τα ελκυστικούς στόχους για επιθέσεις. Οι επιπτώσεις μιας επιτυχημένης επίθεσης περιλαμβάνουν διαρροή ιδιωτικών δεδομένων, αλλοίωση μηνυμάτων, μη εξουσιοδοτημένη πρόσβαση σε συσκευές και δυνατότητα πλήρους ελέγχου του οικιακού αυτόματου συστήματος.

Οι Naidu και Kumar (2019) τονίζουν ότι παρά την ευρεία χρήση των παραπάνω πρωτοκόλλων, η ασφάλειά τους ποικίλλει σημαντικά λόγω διαφορετικών αρχιτεκτονικών, συχνοτήτων λειτουργίας και μηχανισμών κρυπτογράφησης. Το Wi-Fi, για παράδειγμα, προσφέρει υψηλές ταχύτητες μετάδοσης, αλλά αποτελεί και το πιο στοχευμένο πρωτόκολλο, δεδομένης της μεγάλης του κλίμακας και της ευρείας προσβασιμότητας. Επιθέσεις όπως deauthentication, packet sniffing και brute-force σε ασθενή passwords εξακολουθούν να αποτελούν κοινές απειλές, ειδικά σε περιβάλλοντα όπου χρησιμοποιούνται παλαιότερα πρότυπα ασφαλείας, όπως WEP ή μη επαρκώς υλοποιημένο WPA2. Οι Yadav και Kumar (2022) σημειώνουν ότι η μετάβαση σε WPA3 έχει περιορίσει ορισμένες από αυτές τις ευπάθειες, αλλά η υιοθέτηση παραμένει αργή και πολλά IoT συστήματα συνεχίζουν να χρησιμοποιούν παρωχημένες μορφές ασφάλειας λόγω συμβατότητας.

Αντίθετα με το Wi-Fi, τα πρωτόκολλα Zigbee και Z-Wave έχουν σχεδιαστεί ειδικά για συσκευές χαμηλής κατανάλωσης ενέργειας και δικτυώσεις τύπου mesh. Ωστόσο, η απλότητα του σχεδιασμού τους έχει οδηγήσει σε σημαντικές αδυναμίες. Οι Shahidi (2019) και Danbatta & Varol (2019) αναδεικνύουν ότι τόσο το Zigbee όσο και το Z-Wave παρουσιάζουν προβλήματα στο key management, στην αυθεντικοποίηση συσκευών και στη διαδικασία joining, επιτρέποντας σε έναν επιτιθέμενο να εισαγάγει κακόβουλες συσκευές στο δίκτυο. Μία από τις συχνότερα αναφερόμενες αδυναμίες

του Zigbee είναι η χρήση προεπιλεγμένων παγκόσμιων κλειδιών (global keys), τα οποία όταν διαρρεύσουν επιτρέπουν την αποκρυπτογράφηση των πακέτων. Αυτό σημαίνει ότι ένας εισβολέας μπορεί να υποκλέψει ή να τροποποιήσει δεδομένα, επηρεάζοντας άμεσα την ακεραιότητα της επικοινωνίας.

Παρομοίως, οι Babun et al. (2020) επιδεικνύουν ότι το Zigbee και το Z-Wave μπορούν να υποστούν επιθέσεις παθητικής παρακολούθησης (passive fingerprinting), όπου η ανάλυση των ασύρματων σημάτων επιτρέπει την ταυτοποίηση της συσκευής και των λειτουργικών της χαρακτηριστικών. Αυτό διευκολύνει στοχευμένες επιθέσεις, ιδίως όταν ο εισβολέας σκοπεύει να εκμεταλλευτεί συγκεκριμένα μοντέλα συσκευών με γνωστές ευπάθειες. Αν και η τεχνική fingerprinting δεν αποτελεί επίθεση από μόνη της, λειτουργεί ως κρίσιμο βήμα αναγνώρισης που αυξάνει σημαντικά την αποτελεσματικότητα πιο επιθετικών τεχνικών, όπως spoofing ή replay attacks.

Η αξιοπιστία του Z-Wave αμφισβητείται επίσης. Οι Vattheuer et al. (2023) διαπιστώνουν ότι το Z-Wave, παρά τη σχετική του ωριμότητα, παρουσιάζει ασυνέπειες στην απόδοση και στη σταθερότητα των πακέτων όταν οι συνθήκες λειτουργίας επιβαρύνονται (π.χ. αυξημένες παρεμβολές ή μεγάλος αριθμός κόμβων). Αυτές οι αδυναμίες μπορούν να αξιοποιηθούν από έναν εισβολέα που επιδιώκει είτε να διακόψει την υπηρεσία (DoS) είτε να προκαλέσει λάθος συμπεριφορά συσκευών σε αυτοματισμούς. Επιπλέον, ορισμένες εκδόσεις του Z-Wave έχουν κατηγορηθεί για προβλήματα στην υλοποίηση της S0 και S2 security framework, όπου η ανταλλαγή κλειδιών δεν πραγματοποιείται με ισχυρή προστασία, επιτρέποντας επιθέσεις τύπου man-in-the-middle.

Το Bluetooth, ειδικά στη μορφή Bluetooth Low Energy (BLE), παρουσιάζει διαφορετικό σύνολο αδυναμιών. Οι Varol (2019) και Ab Rahman & Azamuddin (2015) υπογραμμίζουν ότι το BLE λόγω της μικρής εμβέλειας δεν θεωρείται από τους χρήστες ως υψηλού κινδύνου, ωστόσο οι αδυναμίες στο pairing, στη διαδικασία bonding και στη χαλαρή διαχείριση των κλειδιών μπορούν να επιτρέψουν σε έναν επιτιθέμενο να παρακολουθήσει πακέτα (sniffing) ή να εισαγάγει ψευδή μηνύματα. Η επίθεση “BLE spoofing” επιτρέπει σε έναν εισβολέα να προσποιηθεί ότι είναι νόμιμη συσκευή, ενώ η απουσία κρυπτογραφημένης μετάδοσης σε ορισμένες υλοποιήσεις επιτρέπει την παρακολούθηση δεδομένων σε απλό κείμενο.

Η βιβλιογραφία τονίζει ότι τα πρωτόκολλα δεν αντιμετωπίζουν μόνο απειλές από κενά ασφαλείας στον σχεδιασμό τους, αλλά συχνά γίνονται ευάλωτα λόγω αδύναμης ή μη ορθής υλοποίησης. Πολλοί κατασκευαστές συσκευών IoT δεν εφαρμόζουν σωστά τους μηχανισμούς ασφαλείας που παρέχουν τα πρωτόκολλα, είτε για λόγους κόστους είτε για εξοικονόμηση ενέργειας. Οι Coston et al. (2025) αναφέρουν ότι πολλά προβλήματα προκύπτουν από ελλιπή validation, ανύπαρκτους μηχανισμούς ενημέρωσης firmware και απουσία ελέγχων ακεραιότητας στα πακέτα επικοινωνίας.

Σχετικά με τις επιπτώσεις των επιθέσεων, η αλλοίωση μηνυμάτων (message tampering) αποτελεί κρίσιμη απειλή για την ακεραιότητα ενός έξυπνου σπιτιού. Ένας επιτιθέμενος που παρεμβαίνει σε πακέτα Zigbee μπορεί να προκαλέσει ψευδείς ενεργοποιήσεις συσκευών, όπως άναμμα φώτων ή παραπλάνηση αισθητήρων, με σοβαρές συνέπειες για την ασφάλεια και την ιδιωτικότητα. Στο Wi-Fi, η παρεμβολή στην επικοινωνία μπορεί να επιτρέψει την εκκίνηση κακόβουλων ενημερώσεων ή την απόκτηση μη εξουσιοδοτημένης πρόσβασης στον οικιακό router, γεγονός που ανοίγει τον δρόμο για πιο εκτεταμένες παραβιάσεις. Αντίστοιχα, στο Z-Wave και στο Bluetooth οι εισβολείς μπορούν να αναπαράγουν πακέτα (replay attacks), εκτελώντας εντολές όπως ξεκλείδωμα πόρτας ή απενεργοποίηση συστημάτων ασφαλείας.

Όσον αφορά τα προτεινόμενα αντίμετρα, η βιβλιογραφία επισημαίνει την ανάγκη για αυστηρότερη υλοποίηση των πρωτοκόλλων ασφαλείας. Οι Yadav και Kumar (2022) προτείνουν τη χρήση σύγχρονων μεθόδων κρυπτογράφησης, συχνές ενημερώσεις firmware, ισχυρή αυθεντικοποίηση μεταξύ συσκευών και επίβλεψη της κίνησης μέσω intrusion detection συστημάτων για IoT περιβάλλοντα. Παράλληλα, οι Shahidi (2019) υπογραμμίζουν ότι η ασφαλής διαχείριση κλειδιών στο Zigbee και στο Z-Wave αποτελεί προτεραιότητα, με προτάσεις όπως η απενεργοποίηση global keys, η εφαρμογή unique keys ανά συσκευή και η χρήση secure booting.

Οι Danbatta και Varol (2019) σημειώνουν ότι η επιλογή του κατάλληλου πρωτοκόλλου πρέπει να βασίζεται όχι μόνο στην ενεργειακή απόδοση και στην ταχύτητα, αλλά και στις πραγματικές απαιτήσεις ασφάλειας του χώρου. Για παράδειγμα, κρίσιμες συσκευές όπως smart locks ή αισθητήρες ασφάλειας είναι προτιμητέο να βασίζονται σε πρωτόκολλα με αυξημένο επίπεδο προστασίας και αξιόπιστες υλοποιήσεις.

Η βιβλιογραφία καταδεικνύει ότι οι επιθέσεις σε πρωτόκολλα επικοινωνίας αποτελούν έναν από τους σημαντικότερους άξονες κινδύνου στα έξυπνα σπίτια. Παρά τις προόδους στον σχεδιασμό ασφαλέστερων προτύπων, η πραγματική ασφάλεια των πρωτοκόλλων εξαρτάται σε μεγάλο βαθμό από την ποιότητα της υλοποίησης, τη συντήρηση των συσκευών και την αποτελεσματικότητα των μηχανισμών ενημέρωσης.

3.1.3. Διεισδυτικές τεχνικές σε δίκτυα IoT (spoofing, man-in-the-middle, replay attacks)

Τα δίκτυα IoT χαρακτηρίζονται από έντονη ετερογένεια συσκευών, περιορισμένη υπολογιστική ισχύ και ποικιλία πρωτοκόλλων επικοινωνίας, γεγονός που διευρύνει την επιφάνεια επίθεσης και καθιστά εφικτές μια σειρά από διεισδυτικές τεχνικές. Οι επιθέσεις spoofing, man-in-the-middle (MITM) και replay αποτελούν από τις πιο κρίσιμες μορφές παραβίασης, λόγω της ικανότητάς τους να παρακάμπτουν μηχανισμούς αυθεντικοποίησης, να αλλοιώνουν δεδομένα και να επιτρέπουν την πλήρη χειραγώγηση συσκευών χωρίς να γίνονται άμεσα αντιληπτές. Η βιβλιογραφία περιγράφει πειραματικά μοντέλα, προσομοιώσεις και αναλύσεις επιθέσεων που αποδεικνύουν ότι τα υφιστάμενα επίπεδα ασφάλειας των IoT δικτύων είναι συχνά ανεπαρκή για την αντιμετώπιση αυτών των απειλών.

Οι Rajendran et al. (2019) αναφέρουν ότι ο συνδυασμός απουσίας ισχυρών μηχανισμών ταυτοποίησης και η μη αξιοποίηση κρυπτογραφικών προτύπων υψηλής αντοχής ενισχύουν σημαντικά την αποτελεσματικότητα επιθέσεων spoofing. Σε τέτοιες επιθέσεις, ο εισβολέας μιμείται νόμιμη συσκευή και εισάγει ψευδή δεδομένα στο δίκτυο, εκμεταλλευόμενος συχνά πρωτόκολλα χαμηλής κατανάλωσης όπως Zigbee και BLE. Αυτό επιτρέπει τη χειραγώγηση αυτοματισμών, όπως ενεργοποίηση αισθητήρων ή αλλαγή παραμέτρων σε συσκευές ελέγχου περιβάλλοντος. Η απουσία ισχυρών μηχανισμών mutual authentication δημιουργεί ακόμη μεγαλύτερο κίνδυνο, καθώς πολλές IoT συσκευές αποδέχονται δεδομένα από οποιονδήποτε κόμβο εμφανίζεται με έγκυρη δομή πακέτου.

Οι Bazzi et al. (2024) επικεντρώνονται σε επιθέσεις ARP spoofing σε τοπικά δίκτυα που φιλοξενούν IoT συσκευές, δείχνοντας ότι ακόμη και οι πιο βασικές λειτουργίες ενός δικτύου μπορούν να αποτελέσουν εργαλείο MITM επίθεσης. Στη μελέτη τους αποδεικνύεται ότι μέσω παραποίησης της αντιστοίχισης IP-MAC, ένας επιτιθέμενος

μπορεί να τοποθετηθεί αθόρυβα στη μέση της επικοινωνίας δύο συσκευών, αποκτώντας πλήρη ορατότητα στη ροή δεδομένων. Το πρόβλημα επιτείνεται από το γεγονός ότι πολλές IoT συσκευές, ιδιαίτερα χαμηλού κόστους, δεν διαθέτουν μηχανισμούς για την ανίχνευση ασυνήθιστης αλλαγής ARP entries, καθιστώντας τη διείσδυση αόρατη σε επίπεδο χρήστη.

Σε σχέση με τις επιθέσεις MITM, η βιβλιογραφία των τελευταίων ετών καταδεικνύει σημαντική αύξηση των ερευνητικών προσπαθειών για την ανάλυση της λειτουργίας τους και τη μοντελοποίηση της επίδρασής τους στην ακεραιότητα των συστημάτων. Οι Tyagi et al. (2023) εξετάζουν σενάρια MITM που αξιοποιούν την απουσία κρυπτογράφησης σε οικιακά IoT δίκτυα, αποδεικνύοντας ότι ένας εισβολέας μπορεί να εισαγάγει κακόβουλες εντολές σε smart appliances και security devices. Η μελέτη τους δείχνει ότι συσκευές όπως κάμερες, θερμοστάτες και smart locks μπορούν να επηρεαστούν χωρίς ο εισβολέας να χρειαστεί να παραβιάσει το ίδιο το firmware, αλλά αποκτώντας απλώς τη δυνατότητα ανάγνωσης και τροποποίησης πακέτων.

Σε πιο σύγχρονα πλαίσια, οι Fereidouni et al. (2025) προσφέρουν μια εκτεταμένη ανάλυση της φύσης των MITM επιθέσεων σε IoT δίκτυα, υπογραμμίζοντας ότι η αυξανόμενη χρήση cloud-based υπηρεσιών δημιουργεί νέες επιφάνειες επίθεσης. Σύμφωνα με τη μελέτη τους, η μετάβαση από local-only λειτουργίες σε υβριδικά σχήματα cloud-edge-device επιτρέπει την εκμετάλλευση μη ασφαλών APIs, αδύναμων πιστοποιητικών και ελλιπών διαδικασιών επαλήθευσης ταυτότητας server. Αυτό έχει ως αποτέλεσμα επιθέσεις στις οποίες ο εισβολέας παρεμβάλλεται μεταξύ συσκευής και cloud backend, αποκτώντας πρόσβαση σε δεδομένα υψηλής ευαισθησίας ή τροποποιώντας παραμέτρους λειτουργίας.

Αντίστοιχα, οι Tyagi et al. (2024) αναλύουν τις MITM επιθέσεις σε συνδυασμό με τεχνικές DoS, επισημαίνοντας ότι οι δύο μορφές επίθεσης μπορούν να λειτουργήσουν συμπληρωματικά. Για παράδειγμα, μια διαδοχική επίθεση DoS μπορεί να απομονώσει μια συσκευή από τον νόμιμο controller της, ενώ μια MITM επίθεση που εκτελείται ταυτόχρονα επιτρέπει στον εισβολέα να καταλάβει τη θέση του controller. Αυτό καθιστά εφικτό έναν πλήρη έλεγχο συσκευών υψηλής σημασίας, όπως οι μηχανισμοί πρόσβασης και οι αισθητήρες ασφαλείας.

Οι replay attacks αποτελούν άλλη μία κρίσιμη κατηγορία απειλών. Στις επιθέσεις αυτές ο εισβολέας δεν χρειάζεται να κατανοήσει ή να αποκρυπτογραφήσει το περιεχόμενο του πακέτου· αρκεί η καταγραφή ενός έγκυρου πακέτου και η επανάληψή του σε μεταγενέστερο χρόνο. Οι Cherian & Varma (2022) δείχνουν ότι τέτοιες επιθέσεις μπορούν να ενεργοποιήσουν ανεπιθύμητες ενέργειες, όπως το άνοιγμα smart locks ή η απενεργοποίηση συναγερμών, σε συστήματα που δεν διαθέτουν μηχανισμούς anti-replay ή χρονικές υπογραφές. Η μελέτη τους σε SDN-based IoT περιβάλλοντα υπογραμμίζει ότι η ευελιξία των SDN controllers μπορεί να ενισχύσει την άμυνα, αλλά ταυτόχρονα μπορεί να αποτελέσει στόχο εάν ο controller δεν προστατεύεται επαρκώς.

Οι Thankappan et al. (2024) προβαίνουν σε μια από τις πιο προχωρημένες προσομοιώσεις MITM επιθέσεων σε προστατευμένα Wi-Fi δίκτυα, παρουσιάζοντας έναν signature-based μηχανισμό εντοπισμού πολυκαναλικών επιθέσεων. Η έρευνά τους επιβεβαιώνει ότι ακόμη και τα προηγμένα πρότυπα κρυπτογράφησης Wi-Fi μπορούν να υπονομευθούν μέσω τεχνικών MITM που εκμεταλλεύονται το roaming των συσκευών ή το injection αλλοιωμένων beacon frames. Το εύρημα αυτό υπογραμμίζει ότι η ασφάλεια των IoT συσκευών δεν εξαρτάται μόνο από το πρωτόκολλο, αλλά και από το περιβάλλον κινητικότητας και τη συμπεριφορά των συσκευών μέσα στο δίκτυο.

Σε ένα πιο γενικό επίπεδο, οι Cecílio & Souto (2024) εξετάζουν διεισδυτικές τεχνικές σε περιβάλλοντα Industry 4.0, τα οποία μοιράζονται πολλές ομοιότητες με τα οικιακά IoT δίκτυα. Η αναφορά τους σε πολλαπλές MITM επιθέσεις αποδεικνύει ότι οι τεχνικές παραβίασης δεν περιορίζονται σε ένα μόνο σημείο αλλά μπορούν να πραγματοποιηθούν σε διάφορα στρώματα του μοντέλου επικοινωνίας, από φυσικό ως και εφαρμογικό επίπεδο. Μέρος της πρόκλησης, όπως περιγράφουν, είναι ότι πολλές συσκευές εμπιστεύονται χωρίς επαλήθευση την πηγή των δεδομένων που λαμβάνουν, ανοίγοντας δρόμους για spoofing και replay επιθέσεις.

Τέλος, οι Zhraw et al. (2025) προσφέρουν μια χρονολογική και τεχνική επισκόπηση των MITM επιθέσεων, αναλύοντας τις διαχρονικές εξελίξεις, τα αναδυόμενα εργαλεία και τις προκλήσεις στην ανίχνευση. Σύμφωνα με τη μελέτη τους, ένας από τους λόγους που οι MITM επιθέσεις παραμένουν τόσο επιτυχημένες είναι το γεγονός ότι μπορούν να εκτελεστούν είτε παθητικά είτε ενεργά, χωρίς να υπάρχει ομοιογενής μηχανισμός εντοπισμού σε όλα τα πρωτόκολλα IoT. Επιπλέον, η έλλειψη συστηματικής

καταγραφής (logging) σε πολλές συσκευές καθιστά την ακριβή ανάλυση ενός περιστατικού εξαιρετικά δύσκολη.

Οι επιθέσεις spoofing, MITM και replay αποδεικνύονται ιδιαίτερα αποτελεσματικές σε IoT δίκτυα, καθώς εκμεταλλεύονται δομικές αδυναμίες, ελλιπείς μηχανισμούς αυθεντικοποίησης και ανεπαρκείς υλοποιήσεις ασφαλείας. Οι προσομοιώσεις και τα ερευνητικά μοντέλα δείχνουν ότι τα σημερινά μέτρα προστασίας δεν επαρκούν, ειδικά σε συσκευές χαμηλής υπολογιστικής ισχύος. Η ενίσχυση των anti-replay μηχανισμών, η υιοθέτηση mutual authentication, η συνεχής παρακολούθηση δικτυακής κίνησης και η εφαρμογή ολοκληρωμένων intrusion detection συστημάτων προτείνονται ως βασικά μέτρα αντιμετώπισης, αλλά η αποτελεσματικότητά τους εξαρτάται από τη συνεπή και ορθή εφαρμογή τους σε ολόκληρο το IoT οικοσύστημα.

3.1.4. Παραδείγματα πραγματικών περιστατικών και πειραματικών επιθέσεων από τη βιβλιογραφία

Η μελέτη πραγματικών περιστατικών και πειραματικών επιθέσεων σε έξυπνα σπίτια αποτελεί κρίσιμο εργαλείο για την κατανόηση της φύσης των απειλών και των αδυναμιών που ενυπάρχουν στο οικοσύστημα του IoT. Η βιβλιογραφία αναδεικνύει μια σειρά από επιβεβαιωμένες επιθέσεις, εργαστηριακές προσομοιώσεις και case studies που αποκαλύπτουν πόσο ευάλωτες παραμένουν πολλές τεχνολογίες έξυπνων οικιακών συστημάτων. Μέσα από αυτά τα περιστατικά γίνεται εμφανές ότι οι συσκευές και τα πρωτόκολλα επικοινωνίας πάσχουν από ελλείψεις σε σχεδιασμό, μηχανισμούς αυθεντικοποίησης, ενημερώσεις λογισμικού και δυνατότητα έγκαιρης ανίχνευσης ανωμαλιών.

Σε μια από τις πρώτες εκτεταμένες πειραματικές μελέτες, οι Notra et al. (2014) αξιολόγησαν τις ευπάθειες ανερχόμενων οικιακών συσκευών, όπως έξυπνα ψυγεία, θερμοστάτες και κάμερες. Η έρευνά τους κατέδειξε ότι πολλές συσκευές δεν διαθέτουν βασικούς μηχανισμούς ασφαλείας, όπως κρυπτογράφηση δικτυακής κίνησης, ισχυρή αυθεντικοποίηση ή μέτρα αποτροπής firmware tampering. Μέσω πειραματικών επιθέσεων, απέδειξαν τη δυνατότητα υποκλοπής ευαίσθητων δεδομένων, τροποποίησης λειτουργιών συσκευών και ενεργοποίησης παράνομων ενεργειών, όπως άνοιγμα ηλεκτρικών κλειδαριών ή αλλαγή θερμοκρασίας χώρων. Τα αποτελέσματα

υπογράμμισαν ότι ο βασικός σχεδιασμός πολλών συσκευών IoT δεν λαμβάνει υπόψη τις αυξημένες απαιτήσεις κυβερνοασφάλειας.

Ανάλογα συμπεράσματα προέκυψαν και από τους Sivanathan et al. (2017), οι οποίοι διεξήγαγαν συστηματική αξιολόγηση κυβερνοεπιθέσεων σε πραγματικό περιβάλλον smart home. Η μελέτη τους περιλάμβανε ανάλυση της συμπεριφοράς δικτυακής κίνησης, αξιοποίηση τεχνικών spoofing και MITM, καθώς και δοκιμές διείσδυσης σε συσκευές όπως smart TVs, IP cameras, έξυπνους αισθητήρες και οικιακούς hubs. Οι ερευνητές διαπίστωσαν ότι πολλές συσκευές χρησιμοποιούν μη ασφαλή APIs, αδύναμους μηχανισμούς session handling και ελλιπείς διαδικασίες επικύρωσης πακέτων, επιτρέποντας στους επιτιθέμενους να προσομοιώσουν νόμιμες εντολές και να παρακάμψουν πλήρως τα συστήματα ασφαλείας. Επίσης, ανέδειξαν ότι η ανάλυση συμπεριφοράς δικτυακής κίνησης μπορεί να χρησιμοποιηθεί ως μέσο εντοπισμού ανωμαλιών, υπογραμμίζοντας τη σημασία intrusion detection μηχανισμών σε ένα έξυπνο σπίτι.

Εκτός από τα εργαστηριακά πειράματα, ιδιαίτερη σημασία έχουν και οι προσομοιώσεις που εξετάζουν τις επιπτώσεις κυβερνοεπιθέσεων σε πραγματικούς χρήστες. Οι Huijts et al. (2023) διερεύνησαν πώς αντιδρούν οι χρήστες σε simulated cyber-physical attacks στο περιβάλλον ενός έξυπνου σπιτιού. Στο πλαίσιο της μελέτης εφαρμόστηκαν σενάρια όπου έξυπνες συσκευές είτε λειτουργούσαν απρόβλεπτα είτε παρείχαν παραπλανητικές πληροφορίες, προκαλώντας σύγχυση, ανασφάλεια και απώλεια εμπιστοσύνης στα συστήματα IoT. Τα ευρήματα αποκάλυψαν ότι οι χρήστες συχνά δεν είναι σε θέση να αναγνωρίσουν τα σημάδια μιας κυβερνοεπίθεσης και αποδίδουν τη δυσλειτουργία σε τεχνικά σφάλματα. Αυτό τονίζει πως οι επιθέσεις που στοχεύουν στην απορρύθμιση του smart home μπορούν να έχουν σοβαρές ψυχολογικές και λειτουργικές επιπτώσεις, επηρεάζοντας την αντίληψη των χρηστών για την τεχνολογία και τη συμπεριφορά τους απέναντι σε αυτή.

Ιδιαίτερο ενδιαφέρον παρουσιάζουν και οι επιθέσεις που σχετίζονται με την εκτέλεση αυτοματισμών, ειδικά σε πλατφόρμες τύπου IFTTT. Οι Xu et al. (2019) έδειξαν ότι ακόμα και όταν τα δεδομένα μεταδίδονται μέσω κρυπτογραφημένων καναλιών, μπορούν να προκύψουν διαρροές πληροφοριών από τη δομή των εντολών και το περιεχόμενο των κανόνων αυτοματισμού. Η ανάλυσή τους αποκάλυψε ότι ένας

επιτιθέμενος μπορεί, χωρίς να έχει πλήρη πρόσβαση στις συσκευές, να εξαγάγει πληροφορίες για τις συνήθειες των χρηστών, την παρουσία τους στον χώρο και τον τρόπο που έχουν διαμορφώσει τους αυτοματισμούς τους. Το εύρημα αυτό αναδεικνύει ότι οι επιθέσεις δεν απαιτούν πάντα πρόσβαση στη συσκευή, αλλά μπορούν να προκύψουν από την ανάλυση του τρόπου λειτουργίας της.

Σε επίπεδο συστημικών προκλήσεων, οι Komninos et al. (2014) διεξάγουν μια εκτενή επισκόπηση των περιστατικών ασφαλείας σε smart grid και smart home συστήματα. Η ανασκόπησή τους παραθέτει πληθώρα παραδειγμάτων όπου εισβολείς κατάφεραν να τροποποιήσουν δεδομένα που σχετίζονται με την κατανάλωση ενέργειας, να αλλάξουν λειτουργίες smart meters ή να εκμεταλλευτούν αδύναμα επικοινωνιακά πρωτόκολλα. Τα περιστατικά αυτά αποκαλύπτουν ότι τα ενεργειακά συστήματα αποτελούν κρίσιμους στόχους, τόσο λόγω του οικονομικού τους ρόλου όσο και λόγω της δυνατότητας πρόκλησης κοινωνικής αναστάτωσης μέσω εκτεταμένων δυσλειτουργιών.

Οι Xenofontos et al. (2021) παρουσιάζουν μια πλούσια συλλογή case studies που περιλαμβάνουν επιθέσεις σε οικιακές, εμπορικές και βιομηχανικές IoT εγκαταστάσεις. Σε αρκετές περιπτώσεις, ερευνητικές ομάδες κατάφεραν να αποκτήσουν πρόσβαση σε κάμερες, baby monitors, συστήματα HVAC και άλλες κρίσιμες συσκευές, αξιοποιώντας αδύναμους κωδικούς, μη ασφαλή APIs και προβλήματα στα authentication tokens. Ένα εντυπωσιακό εύρημα της μελέτης τους είναι ότι οι περισσότερες επιθέσεις δεν απαιτούσαν ιδιαίτερη τεχνική κατάρτιση· αντίθετα, βασίζονταν σε απλές τεχνικές σάρωσης και εκμετάλλευσης γνωστών ευπαθειών.

Στο ίδιο πνεύμα, οι Fernandes et al. (2016) ανέδειξαν κρίσιμες αδυναμίες σε emerging smart home εφαρμογές, εξετάζοντας δημοφιλείς πλατφόρμες αυτοματισμού όπως Samsung SmartThings. Η μελέτη αποκάλυψε ότι κακόβουλες εφαρμογές μπορούσαν να αποκτήσουν προνόμια πολύ υψηλότερα από όσα δηλώνονταν στο permission model, επιτρέποντας εντολές όπως ξεκλείδωμα θυρών ή απενεργοποίηση συστημάτων ασφαλείας. Η ερευνητική αυτή ανακάλυψη είχε σημαντικές επιπτώσεις στη βιομηχανία, οδηγώντας σε αναθεωρήσεις των permission frameworks.

Το ζήτημα της έγκαιρης ανίχνευσης επιθέσεων αναδεικνύεται μέσα από τη δουλειά των Anthi et al. (2019), οι οποίοι ανέπτυξαν ένα supervised intrusion detection σύστημα

ειδικά για smart homes. Χρησιμοποιώντας δεδομένα από πραγματικές συσκευές, το σύστημα κατάφερε να εντοπίσει ανωμαλίες που υποδήλωναν επιθέσεις MITM, spoofing και malware, αποδεικνύοντας ότι συστήματα συμπεριφορικής ανάλυσης μπορούν να βελτιώσουν σημαντικά το επίπεδο προστασίας.

Εξίσου σημαντικές είναι οι μελέτες που αξιολογούν πειραματικές λύσεις άμυνας. Οι Addison et al. (2025) παρουσίασαν ένα χαμηλού κόστους σύστημα threat intelligence, το οποίο αντλεί δεδομένα σε πραγματικό χρόνο από IoT συσκευές και εντοπίζει ύποπτες ενέργειες όπως απότομη αύξηση traffic, μη αναμενόμενα patterns πρόσβασης και μη εξουσιοδοτημένες αλλαγές firmware. Η αξιολόγηση της λύσης έδειξε ότι ακόμα και περιορισμένης υπολογιστικής ισχύος συσκευές μπορούν να υποστηρίξουν λειτουργίες βασικού επιπέδου ανίχνευσης απειλών.

Ορισμένα case studies επικεντρώνονται σε ειδικές κατηγορίες αυτοματισμών. Οι Khoa et al. (2020) ανέλυσαν την ασφάλεια ενός IoT smart lighting συστήματος, δείχνοντας ότι ήταν εφικτό να διακοπεί ή να τροποποιηθεί η λειτουργία του μέσω επιθέσεων που στοχεύουν στην παραποίηση των πακέτων φωτισμού. Οι ερευνητές απέδειξαν ότι ο χειρισμός του φωτισμού μπορεί να χρησιμοποιηθεί όχι μόνο για πρόκληση αναστάτωσης, αλλά και ως μέσο gathering information για την παρουσία και τις συνήθειες των χρηστών.

Τέλος, οι Mosenia et al. (2017) εισήγαγαν το πλαίσιο DISASTER, το οποίο αποδεικνύει πώς οι επιτιθέμενοι μπορούν να στοχεύσουν αισθητήρες που ενεργοποιούν emergency systems. Μέσω έξυπνων τεχνικών spoofing, κατάφεραν να ενεργοποιήσουν ψευδείς συναγερμούς ή να απενεργοποιήσουν κρίσιμα συστήματα, καταδεικνύοντας τους σοβαρούς κινδύνους που μπορεί να προκύψουν από την εκμετάλλευση των αισθητήρων ενός smart home.

Η συνολική ανάλυση των παραπάνω περιστατικών καταδεικνύει ότι οι κυβερνοεπιθέσεις σε smart homes δεν αποτελούν θεωρητικό σενάριο, αλλά πρακτική πραγματικότητα. Οι αδυναμίες εκτείνονται από επιφανειακά θέματα σχεδιασμού μέχρι βαθιά συστημικά προβλήματα σε πρωτόκολλα και αυτοματισμούς. Παρά τις προόδους στις λύσεις προστασίας, η συστηματική αποτίμηση δείχνει ότι απαιτείται περαιτέρω έρευνα, τυποποίηση και ενίσχυση του οικοσυστήματος, ώστε να περιοριστούν οι ευρείες και δυνητικά επικίνδυνες συνέπειες των επιθέσεων.

3.2 Σύγχρονες προσεγγίσεις για την ενίσχυση της ασφάλειας IoT

Παράλληλα με την ανάλυση των επιθέσεων, η βιβλιογραφία έχει προτείνει πληθώρα τεχνικών και αρχιτεκτονικών προσεγγίσεων για την ενίσχυση της ασφάλειας στα έξυπνα σπίτια. Οι προσεγγίσεις αυτές καλύπτουν διαφορετικά επίπεδα: από αρχιτεκτονικές λύσεις και gateways μέχρι μηχανισμούς αυθεντικοποίησης, κρυπτογράφησης, risk assessment και χρήση νέων τεχνολογιών, όπως το blockchain και η τεχνητή νοημοσύνη.

Ένα χαρακτηριστικό παράδειγμα αρχιτεκτονικής προσέγγισης αποτελεί η εργασία των Dorri et al., οι οποίοι προτείνουν μια αρχιτεκτονική βασισμένη σε blockchain για την ασφάλεια και την ιδιωτικότητα στο έξυπνο σπίτι (Dorri et al., 2017). Στην πρότασή τους, οι συσκευές δεν επικοινωνούν απευθείας με το δημόσιο blockchain, αλλά μέσω ενός τοπικού hub, μειώνοντας σημαντικά το κόστος και την πολυπλοκότητα. Τα πειραματικά αποτελέσματα δείχνουν ότι η προσθήκη του blockchain δεν επιβαρύνει υπερβολικά την απόδοση: ο χρόνος επεξεργασίας ανά συναλλαγή παραμένει κάτω από τα 80 ms, ενώ η επιπλέον κατανάλωση ενέργειας είναι της τάξης του 0,01 mJ ανά συναλλαγή, ποσοστό που αντιστοιχεί σε ελάχιστη αύξηση σε σχέση με την baseline λειτουργία. Τα αριθμητικά αυτά δεδομένα υποδεικνύουν ότι λύσεις που μέχρι πρότινος θεωρούνταν «βαριές» για περιβάλλοντα IoT μπορούν, με κατάλληλη αρχιτεκτονική, να γίνουν πρακτικά εφαρμόσιμες σε έξυπνα σπίτια.

Οι Batalla et al. προσεγγίζουν το πρόβλημα από την πλευρά της ολοκληρωμένης διαχείρισης ασφάλειας σε υποδομές smart home και smart city, προτείνοντας μια αρχιτεκτονική που συνδυάζει μηχανισμούς ασφαλούς δρομολόγησης, πιστοποίησης και διαχείρισης κλειδιών σε πολλαπλά επίπεδα (Batalla et al., 2017). Η έμφαση δίνεται στην ανάγκη τα συστήματα ασφαλείας να είναι ευέλικτα και επεκτάσιμα, ώστε να μπορούν να υποστηρίξουν τον αναμενόμενο πολλαπλασιασμό των συσκευών τα επόμενα χρόνια. Σε πιο «εφαρμοσμένο» επίπεδο, ο Bugeja και οι συνεργάτες του προτείνουν το πλαίσιο PRASH (Privacy Risk Assessment for Smart Homes), το οποίο συνδυάζει τεχνικά δεδομένα τρωτοτήτων και κινδύνων με μετρικές επιπτώσεων για την ιδιωτικότητα (Bugeja et al., 2021). Σύμφωνα με τη μελέτη τους, το PRASH ενσωματώνει κατευθυντήριες γραμμές από υπάρχοντα πλαίσια, όπως το NIST Privacy Framework, αλλά τα επεκτείνει ώστε να λαμβάνουν υπόψη την ιδιαίτερη φύση των

smart homes, όπου οι επιπτώσεις από παραβιάσεις συχνά ξεπερνούν το κλασικό πλαίσιο «διαρροή δεδομένων» και αφορούν τη φυσική παρουσία και τις καθημερινές συνήθειες των ενοίκων. Η εργασία αυτή εδράζεται σε ένα ευρύτερο σώμα εργασιών των ίδιων συγγραφέων σχετικά με μοντέλα απειλών για το smart home και δείχνει ότι η συστηματική ποσοτική αξιολόγηση των κινδύνων –με χρήση μετρικών όπως το CVSS– μπορεί να βοηθήσει τους σχεδιαστές να ιεραρχήσουν αποτελεσματικά τις επενδύσεις σε μέτρα ασφαλείας.

Επιπλέον, οι Dhanraj et al. εξετάζουν, μέσα από συστηματική ανασκόπηση, τους τρόπους με τους οποίους τα έξυπνα κτίρια και σπίτια μπορούν να ενισχύσουν την ασφάλεια και την προστασία της ζωής σε καταστάσεις έκτακτης ανάγκης. Τα αποτελέσματά τους δείχνουν ότι, σε επιλεγμένες μελέτες περιπτώσεων, η υιοθέτηση έξυπνων συστημάτων παρακολούθησης και συναγερμού συνδέθηκε με μείωση συμβάντων κλοπής έως και 60%, μείωση βανδαλισμών έως και 75% και μείωση της τρωτότητας σε διαρρήξεις της τάξης του 50% (Dhanraj et al., 2024). Τα αριθμητικά αυτά ευρήματα υποδηλώνουν ότι η σωστή αξιοποίηση των δυνατοτήτων των IoT συσκευών μπορεί να έχει απτά οφέλη στην ασφάλεια του φυσικού χώρου, υπό την προϋπόθεση ότι συνοδεύεται από επαρκή τεχνικά και οργανωτικά μέτρα ασφαλείας.

Στον χώρο των ιατρικών εφαρμογών, η μελέτη των Harvey et al. εστιάζει στην ασφάλεια των Medical IoT (MIoT) συσκευών μέσα στο έξυπνο σπίτι, προτείνοντας μια αρχιτεκτονική που λαμβάνει υπόψη την ετερογένεια των συσκευών και των πρωτοκόλλων επικοινωνίας (Harvey et al., 2020). Οι συγγραφείς επισημαίνουν ότι ο αυξανόμενος αριθμός MIoT συσκευών σε οικιακά περιβάλλοντα –ιδιαίτερα σε σενάρια τηλεϊατρικής και απομακρυσμένης παρακολούθησης ασθενών– εντείνει την ανάγκη για ισχυρούς μηχανισμούς αυθεντικοποίησης, κρυπτογράφησης και διαχωρισμού δικτύου, καθώς τυχόν παραβίαση δεν απειλεί μόνο την ιδιωτικότητα αλλά και τη ζωή του ασθενούς.

Από την πλευρά της χωρικής και λειτουργικής αρχιτεκτονικής των smart homes, ο Mocrii και οι συνεργάτες του αναλύουν σενάρια όπου εκατοντάδες αισθητήρες και ενεργοποιητές συνδέονται σε μια ενιαία πλατφόρμα, υπογραμμίζοντας την ανάγκη για κεντρική διαχείριση ασφάλειας, αλλά και για μηχανισμούς αυτοδιάγνωσης και αυτόματης ανάκαμψης από αστοχίες (Mocrii et al., 2018). Αντίστοιχα, ο Renu

παρουσιάζει διάφορα μοντέλα έξυπνων σπιτιών, εξηγώντας πώς οι διαφορετικές τοπολογίες (π.χ. πλήρως αποκεντρωμένες ή υβριδικές με firewall/gateway) επηρεάζουν την έκθεση σε επιθέσεις και τις απαιτήσεις για μηχανισμούς ασφαλείας (Renu, 2019).

Σημαντική είναι, επίσης, η συμβολή των πλαισίων για ανάλυση και μοντελοποίηση κινδύνων. Εκτός από το PRASH, η βιβλιογραφία περιλαμβάνει εργαλεία όπως το IoTRiskAnalyzer, μορφές μοντελοποίησης σε attack trees και προσεγγίσεις που αξιοποιούν model checking για την αξιολόγηση της πιθανότητας παραβίασης συγκεκριμένων σεναρίων. Οι Bugeja et al. επισημαίνουν ότι τέτοια εργαλεία επιτρέπουν στους ερευνητές να συνδέσουν τρωτότητες που εντοπίζονται σε βάσεις δεδομένων όπως το NVD με συγκεκριμένες έξυπνες συσκευές και αυτοματισμούς, ώστε να εκτιμηθεί αριθμητικά η πιθανότητα και η σοβαρότητα μιας επίθεσης στο οικιακό περιβάλλον (Bugeja et al., 2021).

Τέλος, οι νεότερες εργασίες των Magara και Zhou, καθώς και των Albayaydh et al., στρέφουν το βλέμμα προς την αξιοποίηση της τεχνητής νοημοσύνης για την ενίσχυση της ασφάλειας και της ιδιωτικότητας στα smart homes. Οι Magara και Zhou επισημαίνουν ότι, σε έναν κόσμο με δεκάδες δισεκατομμύρια συνδεδεμένες συσκευές, η παρακολούθηση ανωμαλιών σε πραγματικό χρόνο και η δυναμική εφαρμογή πολιτικών ασφαλείας είναι πρακτικά αδύνατο να γίνουν μόνο από τον άνθρωπο, καθιστώντας τους αλγορίθμους μηχανικής μάθησης απαραίτητους για την ανίχνευση ασυνήθιστων μοτίβων συμπεριφοράς (Magara & Zhou, 2024). Αντίστοιχα, οι Albayaydh et al. διερευνούν πώς τα συστήματα γενετικής ΤΝ μπορούν να βοηθήσουν τους χρήστες –και ειδικά ευάλωτες ομάδες, όπως ηλικιωμένους– να κατανοήσουν και να διαχειριστούν τις ρυθμίσεις ιδιωτικότητας με πιο φιλικό τρόπο, προτείνοντας ευφυείς βοηθούς που εξηγούν επιλογές και συνέπειες.

Οι σύγχρονες προσεγγίσεις για την ενίσχυση της ασφάλειας στα smart homes δείχνουν μια μετάβαση από αποσπασματικές λύσεις (π.χ. μεμονωμένη κρυπτογράφηση ή firewall) σε ολιστικά πλαίσια που συνδυάζουν αρχιτεκτονικό σχεδιασμό, ανάλυση κινδύνων, αυτόματη ανίχνευση ανωμαλιών και, ολοένα και περισσότερο, τεχνητή νοημοσύνη.

3.2.1. Μηχανισμοί αυθεντικοποίησης και πρόσβασης (password policies, biometrics, MFA)

Η αυθεντικοποίηση και ο έλεγχος πρόσβασης αποτελούν βασικούς πυλώνες της ασφάλειας στα έξυπνα σπίτια, καθώς λειτουργούν ως η πρώτη γραμμή άμυνας απέναντι σε μη εξουσιοδοτημένη πρόσβαση και παραβίαση των οικιακών IoT συστημάτων. Η μετάβαση από παραδοσιακούς μηχανισμούς βασισμένους σε κωδικούς πρόσβασης προς πιο σύγχρονες τεχνικές, όπως βιομετρικοί έλεγχοι και πολυπαραγοντική αυθεντικοποίηση (MFA), αντανακλά την ανάγκη για ενίσχυση της ασφάλειας σε ένα περιβάλλον όπου οι συσκευές είναι συχνά περιορισμένων πόρων και εκτεθειμένες σε πολλαπλές απειλές. Η βιβλιογραφία αναδεικνύει ότι κάθε μοντέλο αυθεντικοποίησης διαθέτει διαφορετικά πλεονεκτήματα και περιορισμούς, οι οποίοι καθορίζουν τον βαθμό εφαρμοσιμότητάς του στο οικοσύστημα smart home.

Οι πολιτικές κωδικών πρόσβασης (password policies) αποτελούν την πιο διαδεδομένη μορφή ελέγχου πρόσβασης, αλλά και τη λιγότερο ασφαλή όταν δεν εφαρμόζονται σωστά. Οι Mariappan et al. (2025) επισημαίνουν ότι παρά τη μακρόχρονη χρήση τους, οι παραδοσιακοί κωδικοί παραμένουν εξαιρετικά ευάλωτοι σε επιθέσεις brute-force, dictionary attacks, credential stuffing και phishing. Η αδυναμία των χρηστών να δημιουργήσουν ισχυρούς κωδικούς, καθώς και η τάση επαναχρησιμοποίησης ίδιων credentials σε πολλαπλές υπηρεσίες, καθιστούν τις πολιτικές password-based authentication ανεπαρκείς για την προστασία έξυπνων σπιτιών. Επιπλέον, πολλές IoT συσκευές ακόμη λειτουργούν με προεπιλεγμένους εργοστασιακούς κωδικούς, γεγονός που αυξάνει δραματικά τον κίνδυνο παραβίασης.

Σε συγκριτική ανάλυση, οι Abduhari et al. (2025) τονίζουν ότι, παρόλο που η ενίσχυση των password policies –μέσω επιβολής ελάχιστου μήκους, χρήσης πολυπλοκότητας και τακτικής αλλαγής κωδικών– μπορεί να περιορίσει ορισμένες απειλές, ο μηχανισμός παραμένει δομικά αδύναμος. Το βασικό μειονέκτημα έγκειται στο γεγονός ότι η ασφάλεια του συστήματος εξαρτάται από μια ενέργεια που επιτελεί ο χρήστης· και η ανθρώπινη συμπεριφορά έχει αποδειχθεί επανειλημμένα ο πιο εύθραυστος κρίκος της ασφάλειας.

Απέναντι σε αυτές τις αδυναμίες, οι βιομετρικοί μηχανισμοί αυθεντικοποίησης έχουν κερδίσει έδαφος ως μέθοδοι που συνδυάζουν υψηλή ασφάλεια με ευχρηστία. Οι Lipps

et al. (2021) εξετάζουν την εφαρμογή ενός βιομετρικού πολυπαραγοντικού σχήματος αυθεντικοποίησης σε βιομηχανικά IoT περιβάλλοντα, υποδεικνύοντας ότι οι βιομετρικές μέθοδοι (όπως αναγνώριση κίνησης, φωνής ή χειρονομιών) μπορούν να χρησιμοποιηθούν αποτελεσματικά για την ασφαλή ταυτοποίηση χρηστών. Αν και το IIoT διαφέρει από το smart home ως προς την πολυπλοκότητα, πολλά από τα συμπεράσματά τους ισχύουν και για οικιακές εγκαταστάσεις: η δυσκολία αναπαραγωγής βιομετρικών στοιχείων προσφέρει υψηλή προστασία έναντι spoofing, ενώ η άμεση και φυσική διαδικασία αυθεντικοποίησης βελτιώνει τη χρηστικότητα.

Ωστόσο, οι βιομετρικές τεχνικές φέρουν και σοβαρές αδυναμίες. Οι Shukla et al. (2025) σημειώνουν ότι η αποθήκευση βιομετρικών δεδομένων απαιτεί αυστηρά πρωτόκολλα ασφάλειας, καθώς η διαρροή τέτοιων δεδομένων είναι μη αναστρέψιμη. Επιπλέον, σε περιβάλλοντα smart home όπου πολλαπλοί χρήστες έχουν πρόσβαση, η εφαρμογή βιομετρικών ελέγχων μπορεί να οδηγήσει σε θέματα ιδιωτικότητας ή σε σφάλματα ταυτοποίησης. Παρά ταύτα, οι ίδιοι προτείνουν passwordless MFA σχήματα που συνδυάζουν βιομετρία, εγγύτητα συσκευών και contactless communication ως υποσχόμενη λύση που εξαλείφει πλήρως τις αδυναμίες των κωδικών.

Η πολυπαραγοντική αυθεντικοποίηση (MFA) αποτελεί τον πιο ισχυρό και ολοκληρωμένο μηχανισμό προστασίας, ιδιαίτερα σε περιβάλλοντα με πολλαπλές συσκευές και ετερογενείς κινδύνους όπως τα smart homes. Οι Suleski et al. (2023) αναφέρουν ότι η MFA έχει ήδη καθιερωθεί δυναμικά στον χώρο των εφαρμογών Internet of Healthcare Things (IoHT), όπου η ανάγκη προστασίας κρίσιμων δεδομένων είναι μεγάλη. Παρότι το IoHT διαφέρει από το οικιακό IoT, οι τεχνικές MFA μπορούν να μεταφερθούν άμεσα σε έξυπνα σπίτια, όπου η ασφάλεια συχνά παραμένει σε χαμηλότερα επίπεδα. Η χρήση δύο ή περισσότερων παραγόντων –όπως γνώση (password), κατοχή (token, smartphone), ή βιομετρία– μειώνει δραστικά την πιθανότητα επιτυχούς παραβίασης, καθώς ένας εισβολέας θα πρέπει να παρακάμψει πολλαπλά επίπεδα ασφάλειας.

Οι Ali (2022) υποστηρίζουν ότι η MFA αποτελεί κρίσιμο συστατικό για τη θωράκιση της IoT συνδεσιμότητας, ειδικά σε δίκτυα όπου υπάρχουν δημόσια ή ημι-δημόσια σημεία πρόσβασης. Η μελέτη τους δείχνει ότι η υιοθέτηση MFA βοηθά στην αποτροπή επιθέσεων credential theft και session hijacking, δύο συχνών απειλών στα έξυπνα

σπίτια, όπου συσκευές όπως κάμερες, κλειδαριές ή θερμοστάτες επικοινωνούν συνεχώς με cloud υπηρεσίες.

Η σημασία της MFA υπογραμμίζεται και από τους Muthusamy & Sakthi (2025), οι οποίοι παρουσιάζουν τη χρήση της ως «χρυσό κλειδί» για την πρόσβαση σε cloud-based υποδομές. Δεδομένου ότι οι περισσότερες smart home πλατφόρμες βασίζονται σε cloud υπηρεσίες για λειτουργίες αυτοματισμού, αποθήκευσης δεδομένων και remote access, η MFA εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να τροποποιήσουν κρίσιμες παραμέτρους ή να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα. Η ενσωμάτωση MFA επιτρέπει επίσης την ανίχνευση ύποπτης συμπεριφοράς, όπως η προσπάθεια σύνδεσης από άγνωστες συσκευές ή τοποθεσίες.

Εκτός από τη δυσκολία παράκαμψης, η MFA προσφέρει ένα ακόμη σημαντικό πλεονέκτημα: την ανοχή σε σφάλματα. Οι Mariappan et al. (2025) αναφέρουν ότι ακόμη και αν ένας παράγοντας αυθεντικοποίησης παραβιαστεί –όπως ένας κωδικός ή ένα token– οι υπόλοιποι παράγοντες εξακολουθούν να προστατεύουν τη συσκευή. Αυτό έχει ιδιαίτερη σημασία σε smart home περιβάλλοντα όπου η φυσική ασφάλεια δεν μπορεί να θεωρηθεί δεδομένη και μια συσκευή μπορεί να παραβιαστεί ή να κλαπεί.

Αντίστοιχα, οι Shukla et al. (2025) επισημαίνουν ότι οι εξελιγμένες MFA πλατφόρμες μπορούν να λειτουργούν passwordless, μειώνοντας τα προβλήματα που προκύπτουν από την κακή διαχείριση κωδικών. Η αξιοποίηση proximity-based authentication, όπου η παρουσία εξουσιοδοτημένης συσκευής (όπως smartphone) λειτουργεί ως παράγοντας αυθεντικοποίησης, μπορεί να ενισχύσει τη χρηστικότητα χωρίς να θυσιάζει την ασφάλεια.

Ωστόσο, η MFA δεν αποτελεί πανάκεια. Η βιβλιογραφία αναδεικνύει ότι η υλοποίησή της μπορεί να εμφανίσει προβλήματα σε συσκευές χαμηλής ισχύος, οι οποίες δυσκολεύονται να διαχειριστούν πολλαπλούς τύπους αυθεντικοποίησης. Οι Kumar (2025) τονίζουν ότι η επόμενη γενιά συστημάτων πρόσβασης θα πρέπει να βασιστεί σε ελαφριά, ευέλικτα σχήματα αυθεντικοποίησης που δεν επιβαρύνουν την επεξεργαστική ισχύ των IoT συσκευών και ταυτόχρονα παρέχουν ισχυρή ασφάλεια. Απαιτείται επίσης ενιαία προσέγγιση στην αρχιτεκτονική του συστήματος ώστε όλες οι συσκευές να υποστηρίζουν κοινές μορφές αυθεντικοποίησης.

Τέλος, οι Mariappan et al. (2025) και Abduhari et al. (2025) συμφωνούν ότι ο συνδυασμός MFA με role-based access control (RBAC) ή attribute-based access control (ABAC) μπορεί να προσφέρει ακόμη πιο ισχυρή προστασία, επιτρέποντας τον λεπτομερή καθορισμό προνομίων ανά χρήστη ή συσκευή. Στο πλαίσιο ενός έξυπνου σπιτιού, αυτό μπορεί να μεταφραστεί σε περιορισμένη πρόσβαση για παιδιά, επισκέπτες ή προσωρινούς χρήστες, μειώνοντας την πιθανότητα κατάχρησης.

Η σύγκριση των κύριων μηχανισμών αυθεντικοποίησης δείχνει ότι οι παραδοσιακοί κωδικοί, ενώ απλοί και ευρέως διαδεδομένοι, δεν επαρκούν για την ασφάλεια των smart homes. Οι βιομετρικές τεχνικές και ιδιαίτερα η MFA προσφέρουν σημαντικά υψηλότερα επίπεδα προστασίας, υπό την προϋπόθεση ότι υλοποιούνται με ορθό τρόπο και με σεβασμό στα όρια των IoT συσκευών. Η μετάβαση σε passwordless μοντέλα και σε ευφυή πολυπαραγοντικά συστήματα αναδεικνύεται ως η πλέον αποτελεσματική στρατηγική για την ασφάλεια των έξυπνων σπιτιών.

3.2.2. Κρυπτογραφικά πρωτόκολλα και ασφαλής μετάδοση δεδομένων

Η ασφάλεια της μετάδοσης δεδομένων σε έξυπνα σπίτια αποτελεί θεμελιώδη προϋπόθεση για την προστασία της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών που ανταλλάσσονται μεταξύ συσκευών IoT, cloud υπηρεσιών και χρηστών. Καθώς τα έξυπνα σπίτια βασίζονται σε ένα ετερογενές δίκτυο από αισθητήρες, ενεργοποιητές και κεντρικές μονάδες ελέγχου, η ανάγκη για ισχυρά αλλά ταυτόχρονα αποδοτικά κρυπτογραφικά πρωτόκολλα καθίσταται ιδιαίτερα έντονη. Ωστόσο, η περιορισμένη υπολογιστική ισχύς των περισσότερων IoT συσκευών, η μικρή διαθέσιμη μνήμη και η απαίτηση για χαμηλή κατανάλωση ενέργειας δημιουργούν σημαντικές προκλήσεις στην υλοποίηση ισχυρών κρυπτογραφικών μηχανισμών. Η βιβλιογραφία αποδεικνύει ότι η παραδοσιακή κρυπτογραφία, όπως η AES ή τα πλήρη πρωτόκολλα TLS, συχνά υπερβαίνουν τις δυνατότητες μιας συσκευής IoT, οδηγώντας στην ανάγκη για εξειδικευμένες λύσεις lightweight encryption και προηγμένα πρωτόκολλα διαχείρισης κλειδιών.

Οι Dhanda et al. (2020) επισημαίνουν ότι η lightweight κρυπτογραφία σχεδιάστηκε ακριβώς για να καλύψει αυτό το κενό, προσφέροντας μειωμένη υπολογιστική επιβάρυνση και χαμηλότερη κατανάλωση ενέργειας, χωρίς ωστόσο να θυσιάζει την ασφάλεια. Κρυπτογραφικοί αλγόριθμοι ελαφριάς κατηγορίας, όπως οι PRESENT,

SPECK, SIMON και LBlock, έχουν αποδειχθεί κατάλληλοι για συσκευές περιορισμένων πόρων, καθώς απαιτούν ελάχιστη μνήμη και εκτελούνται γρήγορα. Παρά τα πλεονεκτήματά τους, η βιβλιογραφία αναγνωρίζει ότι η μειωμένη πολυπλοκότητα συχνά οδηγεί σε δυνητικές αδυναμίες απέναντι σε εξειδικευμένες επιθέσεις, όπως side-channel analysis και brute-force attacks.

Οι Khan et al. (2020) προσφέρουν μια εκτενή ανάλυση των lightweight κρυπτογραφικών πρωτοκόλλων και τονίζουν ότι η ασφάλειά τους, αν και ικανοποιητική στις περισσότερες περιπτώσεις, εξαρτάται σε μεγάλο βαθμό από τον τρόπο υλοποίησης και τις παραμέτρους λειτουργίας. Ιδιαίτερα, η απουσία σωστών μηχανισμών διαχείρισης κλειδιών (secure key management) αποτελεί μια από τις πιο κρίσιμες αδυναμίες των IoT συστημάτων. Πολλές συσκευές εξακολουθούν να χρησιμοποιούν προεπιλεγμένα κλειδιά ή κλειδιά που είναι hard-coded στο firmware, καθιστώντας την αποκρυπτογράφηση σχετικά απλή διαδικασία για τον επιτιθέμενο.

Οι Sokol et al. (2021) επιβεβαιώνουν ότι οι ελαφριοί κρυπτογραφικοί αλγόριθμοι μπορούν να προσφέρουν ρεαλιστική προστασία σε IoT συστήματα, αλλά προϋποθέτουν σωστό σχεδιασμό στο επίπεδο πρωτοκόλλου. Τονίζουν ότι οι αλγόριθμοι πρέπει να ενσωματώνουν μηχανισμούς για τη δημιουργία ψευδοτυχαίων κλειδιών, αποτροπή επαναχρησιμοποίησης κλειδιών και προστασία από αναπαραγωγή πακέτων (replay attacks). Επιπλέον, προειδοποιούν ότι η kek framework—οι μέθοδοι με τις οποίες αποθηκεύονται, διανέμονται και ανανεώνονται τα κλειδιά—είναι συχνά ανεπαρκής στα περισσότερα smart home οικοσυστήματα.

Οι Naru et al. (2017) προσφέρουν μια από τις πρώτες συστηματικές ανασκοπήσεις της lightweight κρυπτογραφίας στο IoT, τονίζοντας ότι οι περισσότερες υλοποιήσεις εστιάζουν στην κάλυψη βασικών λειτουργικών αναγκών και λιγότερο στις μηχανιστικές απαιτήσεις ασφάλειας. Επισημαίνουν ότι σε πολλές περιπτώσεις η επιλογή του αλγορίθμου γίνεται με βάση τη γρήγορη εκτέλεση και όχι με βάση την αντοχή σε επιθέσεις, οδηγώντας σε συγκρούσεις μεταξύ απόδοσης και ασφάλειας.

Σε πιο πρόσφατη εργασία, οι Singh et al. (2024) αναλύουν προχωρημένους lightweight αλγορίθμους και τονίζουν ότι η επόμενη γενιά κρυπτογραφίας για IoT συσκευές θα πρέπει να υιοθετήσει ένα πολυεπίπεδο μοντέλο. Τέτοιες λύσεις περιλαμβάνουν συνδυασμό συμμετρικής κρυπτογράφησης, hash-based authentication και session keys

που ανανεώνονται δυναμικά, προκειμένου να μειωθεί η πιθανότητα αποκρυπτογράφησης του ίδιου κλειδιού σε μεγάλους όγκους δεδομένων.

Οι Rana et al. (2022) υπογραμμίζουν ότι η lightweight κρυπτογραφία πρέπει να αντιμετωπίσει τρεις κρίσιμες προκλήσεις:

- Περιορισμένη υπολογιστική ισχύς συσκευών IoT, που οδηγεί σε ανάγκη για αλγορίθμους χαμηλής πολυπλοκότητας.
- Ενεργειακούς περιορισμούς, που επιβάλλουν μειωμένη κατανάλωση επειδή πολλές συσκευές λειτουργούν με μπαταρίες.
- Ασυνεπή τυποποίηση, που έχει ως αποτέλεσμα ασυμβατότητες μεταξύ διαφορετικών smart home πλατφορμών.

Οι Goyal et al. (2022) εξετάζουν ειδικά την ενεργειακή απόδοση των ελαφριών κρυπτογραφικών αλγορίθμων και καταλήγουν ότι η ισορροπία μεταξύ ισχύος και ασφάλειας αποτελεί συνεχή πρόκληση. Σε σενάρια όπου η διάρκεια ζωής της μπαταρίας είναι κρίσιμη—όπως σε αισθητήρες πόρτας, ανιχνευτές κίνησης ή συσκευές περιμετρικής ασφάλειας—η χρήση παραδοσιακών κρυπτογραφικών βιβλιοθηκών είναι ανεφάρμοστη. Οι lightweight λύσεις προσφέρουν μια ρεαλιστική εναλλακτική, αλλά απαιτούν ενισχυμένους μηχανισμούς προστασίας κλειδιών για να διασφαλιστεί ότι η μειωμένη πολυπλοκότητα δεν οδηγεί σε προβλήματα ασφάλειας.

Οι Bhardwaj et al. (2017) σημειώνουν ότι, στην πράξη, πολλές IoT επιθέσεις προκύπτουν όχι από την αδυναμία του ίδιου του αλγορίθμου αλλά από κακή υλοποίησή του. Οι προγραμματιστές συχνά παραλείπουν να εφαρμόσουν ασφαλείς πρακτικές, όπως unique key per device, session-level encryption και explicit packet integrity checks. Κατά συνέπεια, οι συσκευές μπορεί να προστατεύονται θεωρητικά από την κρυπτογραφία, αλλά παραμένουν εκτεθειμένες λόγω λανθασμένης ενσωμάτωσης.

Παράλληλα, η έρευνα των Gunathilake et al. (2019) αποκαλύπτει ότι η επόμενη γενιά lightweight κρυπτογραφίας πρέπει να λάβει υπόψη όχι μόνο τεχνικές επιθέσεις αλλά και μελλοντικές απειλές όπως η κβαντική υπολογιστική. Προτείνουν αλγορίθμους που χρησιμοποιούν modular arithmetic, hash-based signatures και composite authentication systems, ώστε να παραμείνουν ανθεκτικοί σε επιθέσεις που προβλέπεται να καταστούν εφικτές στο μέλλον.

Οι Abdulraheem et al. (2020) προτείνουν έναν αποδοτικό lightweight αλγόριθμο ειδικά σχεδιασμένο για IoT περιβάλλοντα, ο οποίος επιτυγχάνει σημαντική μείωση χρήσης ενέργειας και υπολογιστικών πόρων. Η έρευνά τους δείχνει ότι με σωστό σχεδιασμό, οι ελαφριοί αλγόριθμοι μπορούν να προσφέρουν προστασία ίση με παραδοσιακές μεθόδους σε μικρότερη υπολογιστική κλίμακα.

Σε πιο προχωρημένες εφαρμογές, οι Ding et al. (2023) προτείνουν ένα πλήρες πρωτόκολλο ασφαλούς επικοινωνίας για IoT περιβάλλοντα που συνδυάζει lightweight κρυπτογράφηση, mutual authentication και προσαρμοστική διαχείριση κλειδιών. Το πρωτόκολλο αντιμετωπίζει βασικά προβλήματα όπως replay attacks, packet forgery και man-in-the-middle επιθέσεις, αποδεικνύοντας ότι οι λύσεις υψηλής ασφάλειας μπορούν να συμβαδίσουν με τους περιορισμούς των συσκευών.

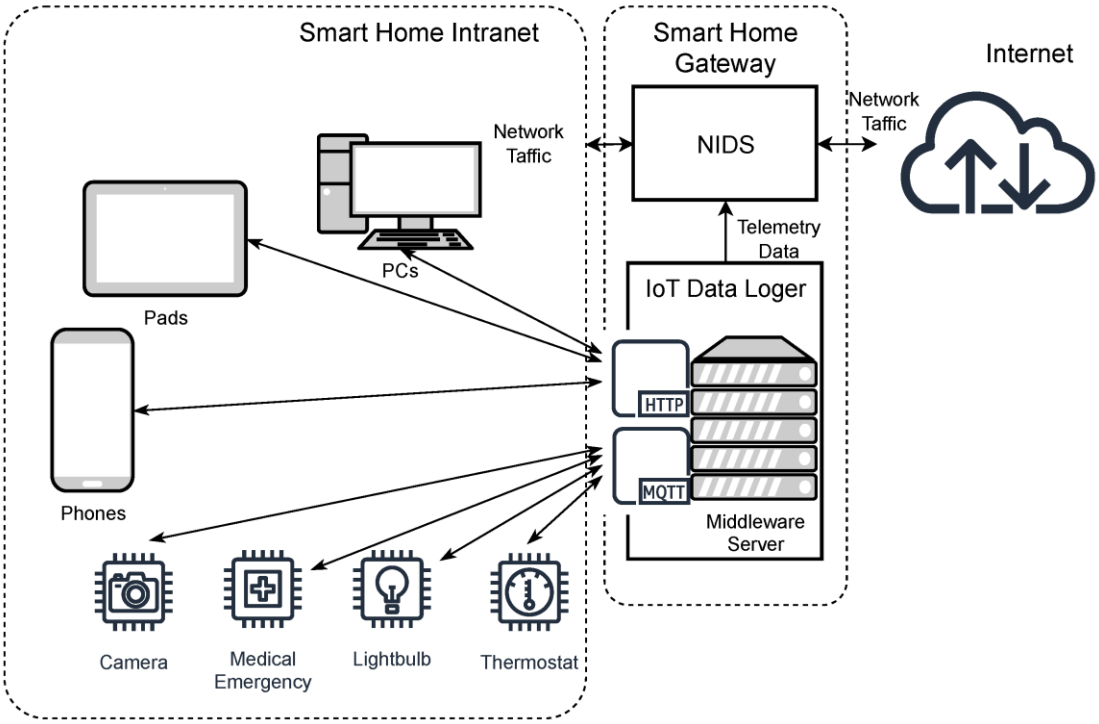
Τέλος, οι Khashan et al. (2021) παρουσιάζουν ένα αυτοματοποιημένο lightweight κρυπτογραφικό σχήμα για ασύρματα αισθητηριακά δίκτυα (WSN), το οποίο επιτυγχάνει σημαντική μείωση κατανάλωσης ενέργειας ενώ ταυτόχρονα ενισχύει την ασφάλεια των πακέτων. Το σχήμα αυτό μπορεί να εφαρμοστεί απευθείας σε smart home περιβάλλοντα, όπου οι αισθητήρες αποτελούν βασικές συσκευές συλλογής δεδομένων.

Η βιβλιογραφία αποκαλύπτει ότι η ασφάλεια της μετάδοσης δεδομένων σε έξυπνα σπίτια βασίζεται σε λεπτή ισορροπία μεταξύ αποδοτικότητας και ισχυρής κρυπτογράφησης. Η lightweight κρυπτογραφία αναδεικνύεται ως η πλέον ρεαλιστική λύση για συσκευές περιορισμένων πόρων, ωστόσο παραμένει σημαντικό να ενισχυθεί με ασφαλή πρωτόκολλα διαχείρισης κλειδιών και σύγχρονες πρακτικές υλοποίησης. Καθώς τα έξυπνα σπίτια εξελίσσονται, η ανάγκη για ισχυρά, ευέλικτα και ενεργειακά αποδοτικά κρυπτογραφικά πρωτόκολλα θα συνεχίσει να αυξάνεται, καθιστώντας την έρευνα στον τομέα αυτόν ιδιαίτερα κρίσιμη.

3.2.3. Τεχνολογίες ανίχνευσης και πρόληψης εισβολών (IDS/IPS για IoT περιβάλλοντα)

Η αυξανόμενη υιοθέτηση έξυπνων συσκευών σε οικιακά IoT περιβάλλοντα έχει οδηγήσει στη διεύρυνση της επιφάνειας επίθεσης, καθιστώντας τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS) ιδιαίτερα κρίσιμα για την προστασία

της ακεραιότητας και της διαθεσιμότητας των υπηρεσιών. Τα IDS/IPS συστήματα έχουν σχεδιαστεί ώστε να εντοπίζουν ανωμαλίες, κακόβουλες ενέργειες ή απόπειρες παραβίασης μέσα στο δίκτυο, λειτουργώντας είτε παθητικά μέσω παρακολούθησης της κίνησης είτε ενεργά, παρεμβαίνοντας για την αποτροπή της επίθεσης. Η εφαρμογή αυτών των τεχνολογιών σε IoT περιβάλλοντα παρουσιάζει ιδιαίτερες δυσκολίες λόγω των περιορισμών σε υπολογιστική ισχύ, ενέργεια και μνήμη, καθώς και λόγω της ετερογένειας των συσκευών.



Εικόνα 6. Παράδειγμα αρχιτεκτονικής έξυπνου σπιτιού με ενσωματωμένο σύστημα ανίχνευσης εισβολών δικτύου (NIDS) και middleware για συσκευές IoT. Πηγή: (Wang et al., 2023).

Στην Εικόνα 6 παρουσιάζεται ένα ενδεικτικό σενάριο έξυπνου σπιτιού με ενσωματωμένο σύστημα ανίχνευσης εισβολών δικτύου (Network Intrusion Detection System – NIDS). Η αρχιτεκτονική βασίζεται σε έναν κεντρικό κόμβο (smart home gateway), ο οποίος συνδυάζει λειτουργίες middleware και μηχανισμούς παρακολούθησης της δικτυακής κίνησης και των τηλεμετρικών δεδομένων των

συσκευών IoT. Μέσω πρωτοκόλλων όπως τα MQTT και HTTP, τα δεδομένα συλλέγονται, επεξεργάζονται και αναλύονται, επιτρέποντας την έγκαιρη ανίχνευση κακόβουλων ή ανώμαλων συμπεριφορών στο οικιακό δίκτυο.

Οι Kumar et al. (2022) εξετάζουν ολοκληρωμένα ένα σύστημα IDS/IPS προσαρμοσμένο για IoT περιβάλλοντα, επισημαίνοντας ότι η κύρια πρόκληση έγκειται στην ανάγκη για lightweight αρχιτεκτονικές που μπορούν να λειτουργήσουν αποδοτικά σε συσκευές χαμηλών πόρων. Η μελέτη τους δείχνει ότι η υλοποίηση ενός IDS/IPS σε smart home υποδομές πρέπει να ισορροπεί μεταξύ ακρίβειας ανίχνευσης και περιορισμένης χρήσης πόρων. Χρησιμοποιώντας υβριδικά μοντέλα (signature-based και anomaly-based), το προτεινόμενο σύστημα καταφέρνει να εντοπίζει γνωστές επιθέσεις ενώ ταυτόχρονα προσφέρει ανίχνευση νέων απειλών μέσω μηχανισμών statistic deviation detection.

Η ανάγκη για ευέλικτες και αποδοτικές αρχιτεκτονικές αναδεικνύεται και στην εργασία του Coulibaly (2020), ο οποίος παρέχει μια ευρεία επισκόπηση των IDS/IPS συστημάτων και των διαφορετικών μοντέλων λειτουργίας τους. Ο συγγραφέας υπογραμμίζει ότι τα signature-based IDS διακρίνονται για την υψηλή ακρίβεια έναντι γνωστών επιθέσεων, αλλά αποτυγχάνουν στην ανίχνευση νέων ή zero-day απειλών. Αντίθετα, τα anomaly-based IDS μπορούν να εντοπίσουν άγνωστες μορφές κακόβουλης δραστηριότητας, αλλά συχνά παράγουν μεγάλο αριθμό false positives, γεγονός που μπορεί να οδηγήσει σε υπερφόρτωση συστημάτων και λανθασμένη απόκριση.

Σε αυτό το πλαίσιο, το Passban IDS που προτείνουν οι Eskandari et al. (2020) αποτελεί χαρακτηριστικό παράδειγμα έξυπνου anomaly-based συστήματος ειδικά σχεδιασμένου για edge IoT συσκευές. Το Passban υλοποιεί αλγορίθμους μηχανικής μάθησης που αναλύουν συνεχώς τη ροή δεδομένων, εντοπίζοντας αποκλίσεις από τη φυσιολογική συμπεριφορά. Οι ερευνητές καταφέρνουν να μειώσουν σημαντικά την υπολογιστική επιβάρυνση μέσω lightweight feature extraction και adaptive learning, καθιστώντας το σύστημα κατάλληλο για περιβάλλοντα περιορισμένων πόρων. Το Passban IDS επιτυγχάνει υψηλό ποσοστό ανίχνευσης (detection rate) και ταυτόχρονα χαμηλό false positive rate, δύο κρίσιμους δείκτες απόδοσης για την αξιολόγηση ενός IDS.

Αντίστοιχα, οι Chiba et al. (2022) παρουσιάζουν μια βαθύτερη ανάλυση σύγχρονων IDS/IPS συστημάτων, αναδεικνύοντας την ανάγκη για συνδυασμό πολλαπλών τεχνικών—όπως deep learning, signature comparison και hybrid anomaly detection—ώστε να αντιμετωπιστεί αποτελεσματικά το συνεχώς εξελισσόμενο τοπίο κυβερνοαπειλών. Σημειώνουν ότι τα IoT περιβάλλοντα απαιτούν όχι μόνο υψηλή ακρίβεια ανίχνευσης, αλλά και ταχεία απόκριση, καθώς πολλές συσκευές έχουν κρίσιμες λειτουργίες στον χώρο του smart home, όπως αισθητήρες ασφαλείας και συστήματα πρόσβασης.

Η έρευνα των Gupta et al. (2023) επιβεβαιώνει ότι ο σχεδιασμός IDS/IPS για IoT πρέπει να ακολουθεί μια αρχιτεκτονική πολυεπίπεδης προστασίας. Οι συγγραφείς αναλύουν πλήθος συστημάτων και καταλήγουν ότι η πιο αποτελεσματική στρατηγική είναι η υλοποίηση IDS τόσο στο edge (near-device processing) όσο και στο cloud, ώστε να επιτυγχάνεται ισορροπία μεταξύ επεξεργαστικής ικανότητας και αμεσότητας στη λήψη αποφάσεων.

Οι Ang et al. (2025) επικεντρώνονται στον τρόπο με τον οποίο η ενσωμάτωση IDS και IPS μπορεί να βελτιώσει σημαντικά τις διαδικασίες παρακολούθησης ασφάλειας. Σύμφωνα με τη μελέτη τους, η χρήση real-time alerting mechanisms και predictive analytics επιτρέπει την άμεση αντίδραση σε ύποπτα συμβάντα, μειώνοντας τον χρόνο εντοπισμού και αποτροπής επιθέσεων. Το εύρημα αυτό είναι ιδιαιτέρως σημαντικό για τα smart homes, όπου μια καθυστέρηση λίγων δευτερολέπτων μπορεί να επιτρέψει σε έναν εισβολέα να εκμεταλλευτεί μια συσκευή, όπως ένα smart lock ή μια κάμερα.

Η συμβολή της μηχανικής μάθησης αναδεικνύεται έντονα στην ανασκόπηση των Jayalaxmi et al. (2022), οι οποίοι μελετούν εκτενώς ML και deep learning μοντέλα για IDS/IPS σε IoT περιβάλλοντα. Τα συστήματα αυτά χρησιμοποιούν τεχνικές όπως convolutional neural networks, autoencoders και recurrent learning για να εντοπίζουν μοτίβα κακόβουλης δραστηριότητας. Παρότι τα deep learning μοντέλα παρουσιάζουν υψηλή ακρίβεια, το κύριο μειονέκτημα είναι η ανάγκη για μεγάλο όγκο δεδομένων εκπαίδευσης και η υψηλή υπολογιστική ζήτηση, η οποία συχνά υπερβαίνει τις δυνατότητες των smart home συσκευών. Ως λύση, οι ερευνητές προτείνουν τη μεταφορά της βαριάς επεξεργασίας στο cloud ή σε τοπικούς edge servers.

Σε άλλη ανασκόπηση, οι Prajapati et al. (2021) αναλύουν πρόσφατες τάσεις IDS/IPS και επιβεβαιώνουν ότι η χρήση cloud-based και hybrid συστημάτων έχει αυξηθεί σημαντικά, καθώς επιτρέπει την υλοποίηση ισχυρών αλγορίθμων ανίχνευσης χωρίς να επιβαρύνονται οι συσκευές IoT. Επισημαίνουν, ωστόσο, ότι η μεταφορά δεδομένων στο cloud αυξάνει την επιφάνεια επίθεσης και απαιτεί ισχυρά πρωτόκολλα κρυπτογράφησης και ασφαλείς διαδικασίες διαχείρισης κλειδιών.

Σε πιο θεωρητικό επίπεδο, ο Möller (2023) τονίζει ότι τα IDS/IPS αποτελούν μία από τις πιο κρίσιμες τεχνολογίες για την κυβερνοασφάλεια στη σύγχρονη ψηφιακή μετάβαση. Αναλύει δείκτες απόδοσης όπως detection latency, sensitivity και false alarm rate, οι οποίοι καθορίζουν το επίπεδο αξιοπιστίας ενός IDS. Για τα IoT περιβάλλοντα, ιδιαίτερη σημασία έχει επίσης η ενεργειακή απόδοση, καθώς η συνεχής παρακολούθηση μπορεί να εξαντλήσει γρήγορα τις μπαταρίες των edge συσκευών.

Οι Jeffrey et al. (2023) επισημαίνουν ότι αν και η έρευνα σε IDS/IPS έχει επικεντρωθεί κυρίως σε βιομηχανικά IoT συστήματα, τα smart home περιβάλλοντα αντιμετωπίζουν παρόμοιες απειλές. Υποστηρίζουν ότι τεχνικές όπως SDN-based IDS μπορούν να μεταφερθούν σε οικιακά δίκτυα, επιτρέποντας δυναμική παρακολούθηση και προσαρμογή κανόνων ασφάλειας.

Οι Rao & Nayak (2014) παρότι παλαιότερης χρονολογίας, παρέχουν θεμελιώδη γνώση σχετικά με τη λειτουργία των IDS/IPS και τις βασικές κατηγορίες επιθέσεων που πρέπει να αντιμετωπίζουν. Οι αρχές αυτές αποτελούν τη βάση για τον σχεδιασμό των σύγχρονων IoT συστημάτων.

Τέλος, οι Altulaihan et al. (2024) επικεντρώνονται στην ανίχνευση DoS επιθέσεων σε IoT δίκτυα μέσω machine learning algorithms. Η εργασία τους προσφέρει ένα σύστημα anomaly detection με υψηλή ακρίβεια, το οποίο βασίζεται σε ελαφριά μοντέλα και μπορεί να λειτουργήσει χωρίς σημαντική επιβάρυνση σε συσκευές περιορισμένων πόρων.

Η βιβλιογραφία αποδεικνύει ότι τα IDS/IPS είναι απαραίτητα για την ασφαλή λειτουργία ενός smart home, αλλά απαιτούν εξειδικευμένο σχεδιασμό ώστε να ανταποκρίνονται στους περιορισμούς των IoT συσκευών. Η χρήση hybrid αρχιτεκτονικών, η αξιοποίηση ML/AI και η υιοθέτηση efficient anomaly-based

συστημάτων αποτελούν κρίσιμες κατευθύνσεις για την ενίσχυση της προστασίας στο μέλλον.

3.2.4. Προσεγγίσεις βασισμένες σε τεχνητή νοημοσύνη και machine learning

Η τεχνητή νοημοσύνη (AI) και το machine learning (ML) έχουν αναδειχθεί ως βασικοί μοχλοί ενίσχυσης της ασφάλειας στα IoT περιβάλλοντα, καθώς προσφέρουν δυνατότητες αυτόματης ανίχνευσης ανωμαλιών, πρόβλεψης επιθέσεων, ενίσχυσης της αυθεντικοποίησης και ταχύτερης απόκρισης σε κυβερνοαπειλές. Οι παραδοσιακές τεχνικές ασφαλείας, όπως ο απλός έλεγχος υπογραφών (signature-based detection), αποδεικνύονται ανεπαρκείς για την αντιμετώπιση των σύγχρονων επιθέσεων που εξελίσσονται συνεχώς, ιδίως σε έξυπνα σπίτια όπου συνυπάρχουν δεκάδες ετερογενείς συσκευές με διαφορετικούς πόρους και προφίλ κινδύνου. Η βιβλιογραφία αποκαλύπτει μια ποικιλία μοντέλων και μεθοδολογιών AI/ML που επιχειρούν να προσφέρουν προσαρμοστικές και υψηλής ακρίβειας λύσεις ασφάλειας, αλλά παράλληλα αναδεικνύει και σημαντικούς περιορισμούς και προκλήσεις.

Οι Rafique et al. (2024) τονίζουν ότι οι σύγχρονες τεχνικές ML και deep learning (DL) για ανίχνευση ανωμαλιών αποτελούν την πιο δραστήρια περιοχή έρευνας στο IoT security. Ένα από τα βασικά πλεονεκτήματα αυτών των προσεγγίσεων είναι ότι μπορούν να εντοπίσουν επιθέσεις που δεν έχουν εμφανιστεί ξανά στο παρελθόν—ιδιαίτερα σημαντικό δεδομένης της πληθώρας zero-day exploits που στοχεύουν IoT συσκευές. Ωστόσο, οι συγγραφείς επισημαίνουν ότι η επιτυχία των ML/DL συστημάτων εξαρτάται σε μεγάλο βαθμό από την ποιότητα των δεδομένων εκπαίδευσης, κάτι που στα IoT περιβάλλοντα δεν είναι πάντοτε δεδομένο, λόγω noisiness, ετερογένειας και έλλειψης labels.

Εστιάζοντας στις τεχνικές anomaly detection, οι Alsalman (2024) συγκρίνει διάφορα ML μοντέλα που χρησιμοποιούνται για τον εντοπισμό επιθέσεων σε IoT δίκτυα. Τα adaptive ML συστήματα που εξετάζει αποδεικνύονται ικανά να προσαρμόζονται σε μεταβαλλόμενες συνθήκες, μειώνοντας τα false positives που αποτελούν πάγιο πρόβλημα των anomaly-based συστημάτων. Η ευελιξία αυτή είναι ιδιαίτερα σημαντική για τα smart homes, όπου οι συνήθειες των χρηστών μεταβάλλονται συχνά, με αποτέλεσμα τα στατικά μοντέλα να αποτυγχάνουν.

Οι Abusitta et al. (2023) προτείνουν deep learning-enabled συστήματα ανίχνευσης που χρησιμοποιούν εξελιγμένες αρχιτεκτονικές—όπως LSTM και CNN layers—για την πρόβλεψη κακόβουλης συμπεριφοράς με υψηλή ακρίβεια. Τα DL μοντέλα υπερτερούν των απλών ML αλγορίθμων καθώς μπορούν να μαθαίνουν πολύπλοκα μοτίβα χωρίς εκτεταμένη προεπεξεργασία. Ωστόσο, η υπολογιστική τους απαίτηση είναι σημαντική, κάτι που περιορίζει τη δυνατότητα υλοποίησης τους απευθείας σε IoT συσκευές χαμηλής ισχύος. Για αυτόν τον λόγο, οι συγγραφείς υποστηρίζουν υλοποιήσεις edge-enhanced DL, όπου μέρος της επεξεργασίας εκτελείται σε edge servers ή gateways.

Το θέμα της κατανομής υπολογιστικών πόρων αναδεικνύεται έντονα στη μελέτη των Mothukuri et al. (2021), οι οποίοι παρουσιάζουν ένα federated learning σύστημα για την ανίχνευση ανωμαλιών. Το μοντέλο αυτό επιτρέπει στις συσκευές να εκπαιδεύουν τοπικά μοντέλα ML χωρίς να αποστέλλουν raw data στο cloud, μειώνοντας τον κίνδυνο διαρροής ευαίσθητων πληροφοριών. Η federated προσέγγιση αποδεικνύεται ιδιαίτερα χρήσιμη για smart home περιβάλλοντα όπου η ιδιωτικότητα των χρηστών είναι υψίστης σημασίας. Παρά τα πλεονεκτήματα, οι συγγραφείς αναγνωρίζουν ότι το federated learning απαιτεί συγχρονισμό και σημαντικό όγκο επικοινωνίας μεταξύ συσκευών, κάτι που μπορεί να επιβαρύνει περιορισμένα IoT δίκτυα.

Οι Kumar et al. (2025) προτείνουν ένα υβριδικό deep learning μοντέλο που συνδυάζει CNN και RNN layers για ανίχνευση ανωμαλιών σε IoT περιβάλλοντα. Το μοντέλο αυτό έχει τη δυνατότητα να καταγράφει τόσο χωρικά όσο και χρονικά μοτίβα επιθέσεων, επιτυγχάνοντας υψηλά ποσοστά detection accuracy. Η μελέτη επιβεβαιώνει ότι τα υβριδικά DL συστήματα υπερτερούν των μονοδιάστατων αλγορίθμων, αλλά απαιτούν προσεκτικό tuning υπερπαραμέτρων για να αποφευχθεί το overfitting.

Αντίστοιχα, οι Ullah & Mahmoud (2021) αναπτύσσουν ένα deep learning framework που αξιοποιεί autoencoders και dense neural network layers για την αυτόματη κατηγοριοποίηση δικτυακών επιθέσεων. Το σύστημα παρουσιάζει υψηλό recall και μπορεί να εντοπίζει πολύ μικρές αποκλίσεις στην κυκλοφορία ενός IoT δικτύου, γεγονός που το καθιστά χρήσιμο για smart home εφαρμογές όπως έλεγχος πρόσβασης, ανίχνευση κακόβουλης συσκευής και προστασία από MITM επιθέσεις.

Η μελέτη του Abid (2023) επικεντρώνεται στην εφαρμογή supervised ML για ταξινόμηση επιθέσεων και αποδεικνύει ότι ακόμη και «ελαφριά» μοντέλα όπως

Random Forest και Gradient Boosting μπορούν να επιτύχουν υψηλή ακρίβεια σε IoT περιβάλλοντα όταν τροφοδοτούνται με προσεκτικά επιλεγμένα χαρακτηριστικά (features). Αυτό αποτελεί ιδιαίτερα σημαντικό εύρημα, καθώς οι συσκευές smart home συχνά δεν μπορούν να υποστηρίξουν περίπλοκα DL μοντέλα.

Οι Gudala et al. (2019) εξετάζουν τη χρήση AI για αυτοματοποιημένη ανίχνευση απειλών σε resource-constrained IoT συστήματα, παρουσιάζοντας τεχνικές optimization και pruning που μειώνουν σημαντικά το computational cost των ML μοντέλων. Αυτό επιτρέπει την υλοποίηση τους ακόμη και σε low-end συσκευές, δημιουργώντας προϋποθέσεις για ευρεία εφαρμογή AI-based ασφάλειας σε έξυπνα σπίτια.

Οι Khan & Alkhathami (2024) επιβεβαιώνουν ότι οι ML μέθοδοι μπορούν να ενισχύσουν δραστικά την πρόβλεψη επιθέσεων σε IoT περιβάλλοντα με ευαίσθητα δεδομένα, όπως αυτά των smart healthcare συστημάτων. Τα ευρήματά τους μεταφέρονται εύκολα στα smart homes, όπου η έγκαιρη ανίχνευση ανωμαλιών σε συσκευές όπως κάμερες και αισθητήρες είναι κρίσιμη για την αποτροπή επιθέσεων.

Οι Wajid & Sans (2024) τονίζουν ότι η αυτοματοποίηση της άμυνας μέσω AI απαιτεί τη δημιουργία feedback-driven security συστημάτων, τα οποία μπορούν να λαμβάνουν αποφάσεις real-time, όπως απομόνωση συσκευής ή αλλαγή διαδρομής επικοινωνίας. Η πλήρης αυτοματοποίηση, ωστόσο, παρουσιάζει προκλήσεις, αφού απαιτεί υψηλό επίπεδο εμπιστοσύνης στα μοντέλα και μηχανισμούς που αποτρέπουν εσφαλμένες ενέργειες (false-action risks).

Σε μια από τις πλέον ολοκληρωμένες ανασκοπήσεις, οι Diro et al. (2021) συνοψίζουν τα ML-based anomaly detection schemes και καταγράφουν ότι η μεγαλύτερη πρόκληση παραμένει η επίτευξη ισορροπίας μεταξύ ακρίβειας, ταχύτητας και ελαχιστοποίησης των false positives. Επίσης, υπογραμμίζουν ότι η έλλειψη τυποποίησης στα IoT δεδομένα αποτελεί σημαντικό εμπόδιο για την καθολική εφαρμογή ML λύσεων.

Οι Jangam & Muntala (2022) εξετάζουν τις εφαρμογές AI και ML στη συνολική ασφάλεια των IoT συσκευών, τονίζοντας ότι πέρα από ανίχνευση ανωμαλιών, οι τεχνικές αυτές μπορούν να ενισχύσουν την αυθεντικοποίηση (π.χ. μέσω behavioral

biometrics), να προβλέψουν επιθέσεις authentication bypass και να βελτιστοποιήσουν την κατανομή πόρων ασφαλείας.

Παρά τα πλεονεκτήματά τους, οι προσεγγίσεις AI/ML αντιμετωπίζουν σοβαρές προκλήσεις. Οι κυριότερες είναι:

- Υψηλές υπολογιστικές απαιτήσεις για DL μοντέλα.
- Ανάγκη για ποιοτικά datasets, τα οποία συχνά δεν υπάρχουν σε οικιακά περιβάλλοντα.
- Κίνδυνος overfitting, που μειώνει την πραγματική αποτελεσματικότητα ενός μοντέλου.
- Ευπάθεια σε adversarial attacks, όπου μικρές μεταβολές στα δεδομένα μπορούν να εξαπατήσουν τα μοντέλα.
- Ζητήματα ιδιωτικότητας, ειδικά όταν τα δεδομένα αποστέλλονται σε cloud για εκπαίδευση.

Η βιβλιογραφία αναδεικνύει ότι οι AI/ML τεχνικές αποτελούν τον πιο υποσχόμενο δρόμο για την ενίσχυση της ασφάλειας στα smart homes, αλλά απαιτούν στοχευμένη υλοποίηση, εφικτή ενεργειακή κατανάλωση και αυστηρούς μηχανισμούς προστασίας της ιδιωτικότητας.

3.2.5. Αρχιτεκτονικές ασφαλούς σχεδιασμού (secure-by-design, privacy-by-design)

Η έννοια του ασφαλούς σχεδιασμού (secure-by-design) και της ιδιωτικότητας από τον σχεδιασμό (privacy-by-design) αποτελεί πλέον θεμελιώδη αρχή για τα σύγχρονα συστήματα IoT και ιδίως για τα έξυπνα σπίτια, όπου η συνεχής συλλογή δεδομένων και η αδιάλειπτη λειτουργία συσκευών δημιουργούν ενισχυμένους κινδύνους ασφάλειας και ιδιωτικότητας. Η βιβλιογραφία δείχνει ότι η ενσωμάτωση των αρχών αυτών από το πρώτο στάδιο ανάπτυξης μειώνει δραστικά την έκθεση σε απειλές, ενώ παράλληλα ενισχύει τη συμμόρφωση με ρυθμιστικά πλαίσια και βέλτιστες πρακτικές. Η μετάβαση από παραδοσιακές αντιδραστικές προσεγγίσεις ασφάλειας προς προληπτικές, δομικές αρχιτεκτονικές απαιτεί συστηματικό σχεδιασμό, αξιολόγηση κινδύνων και εφαρμογή τεκμηριωμένων μοντέλων απειλών.

Οι Del-Real et al. (2024) συγκρίνουν εκτενώς τα πλαίσια secure-by-design και privacy-by-design μέσω συστηματικής ανασκόπησης, καταλήγοντας ότι παρά τις διαφορετικές τους αφετηρίες, οι δύο προσεγγίσεις συγκλίνουν σε κρίσιμες αρχές όπως η ελαχιστοποίηση δεδομένων, η ενσωμάτωση ελέγχων ασφάλειας στον πυρήνα της αρχιτεκτονικής και η διαρκής επικαιροποίηση βάσει αξιολογήσεων κινδύνου. Η ασφάλεια δεν πρέπει να προβάλλεται ως προαιρετικό προσάρτημα, αλλά ως αναπόσπαστο συστατικό της σχεδίασης των συστημάτων IoT, ιδίως σε smart homes όπου περισσότερες συσκευές έχουν άμεση αλληλεπίδραση με τον καθημερινό τρόπο ζωής των χρηστών.

Σε αντίστοιχη συστηματική ανασκόπηση, οι Del-Real et al. (2025) εξετάζουν τις στρατηγικές, τις αρχές και τα διεθνή πρότυπα που διέπουν την ενσωμάτωση secure-by-design και privacy-by-design πρακτικών στις ψηφιακές τεχνολογίες. Η μελέτη υπογραμμίζει ότι οι σχεδιαστικές αρχές πρέπει να εφαρμόζονται σε όλα τα επίπεδα του κύκλου ζωής ενός προϊόντος, από την αρχική μοντελοποίηση απαιτήσεων μέχρι την ανάπτυξη, δοκιμή, διάθεση και μετέπειτα συντήρηση. Ιδιαίτερη σημασία δίνεται στα compliance frameworks, όπως το GDPR, τα οποία απαιτούν ενσωμάτωση privacy safeguards από το πρώτο στάδιο σχεδιασμού μέσω τεχνικών όπως data minimization, purpose limitation και ενσωματωμένη κρυπτογράφηση.

Ο Jøsang (2024) προσεγγίζει τον secure-by-design σχεδιασμό από τεχνολογική και διακυβερνητική σκοπιά, υπογραμμίζοντας ότι ένα σύστημα ασφαλείας υψηλής αξιοπιστίας πρέπει να ενσωματώνει τρία κύρια συστατικά: επιλογή ασφαλών προεπιλογών (secure defaults), αρχές least privilege και exhaustive threat modeling. Οι αρχές αυτές αποκτούν ιδιαίτερη σημασία στα smart homes, όπου πλήθος συσκευών έρχονται προεγκατεστημένες με αδύναμες ή γενικές ρυθμίσεις ασφαλείας. Ο Jøsang τονίζει ότι ο σχεδιασμός ασφαλών προεπιλογών μπορεί να μειώσει δραστικά την εξάρτηση από τις ικανότητες των χρηστών, οι οποίοι συχνά αγνοούν τις προτεινόμενες πρακτικές ασφαλείας.

Η σημασία του threat modeling αναδεικνύεται και στο έργο των Choudhary et al. (2021), οι οποίοι καταγράφουν εκτενώς τις απειλές, ευπάθειες και αντενέργειες για το οικοσύστημα του IoT. Οι συγγραφείς επισημαίνουν ότι η ανάλυση κινδύνου πρέπει να λαμβάνει υπόψη την ετερογένεια των συσκευών, τη δυναμικότητα των διασυνδέσεων

και την υψηλή πιθανότητα ανθρώπινων σφαλμάτων. Συστήνουν τη χρήση μοντέλων όπως STRIDE και attack trees για την καταγραφή πιθανών διαδρομών επίθεσης και την ενσωμάτωση μέτρων προστασίας σε επίπεδο σχεδιασμού, πριν την υλοποίηση του προϊόντος.

Η φιλοσοφία privacy-by-design αποκτά ιδιαίτερο βάρος στα έξυπνα σπίτια, όπου η συνεχής συλλογή αισθητηριακών δεδομένων μπορεί να αποκαλύψει πρότυπα συμπεριφοράς των χρηστών. Οι Butt et al. (2023) διερευνούν τις προκλήσεις και τις δυνατότητες εφαρμογής privacy-by-design στον χώρο του IoT και επισημαίνουν ότι οι βασικές αρχές—όπως η ελαχιστοποίηση δεδομένων, η αποφυγή υπερβολικής προσωποποίησης και η διαφάνεια στις λειτουργίες επεξεργασίας—είναι κρίσιμες για την αποτροπή προσβολών της ιδιωτικότητας. Η εφαρμογή αυτών των πρακτικών απαιτεί την υιοθέτηση τεχνικών όπως local processing αντί cloud processing όταν αυτό είναι εφικτό, καθώς και την ενσωμάτωση privacy-friendly πρωτοκόλλων αποθήκευσης και μετάδοσης.

Η βιβλιογραφία εξετάζει επίσης την αξιοποίηση προηγμένων τεχνολογιών για την ενίσχυση secure-by-design προσεγγίσεων. Οι Bathalapalli et al. (2025) προτείνουν τη χρήση quantum physical unclonable functions (QPUFs) ως μια καινοτόμο τεχνική security-by-design για το Industrial IoT. Αν και το IoT των έξυπνων σπιτιών έχει μικρότερη ανάγκη βιομηχανικού επιπέδου ανθεκτικότητας, οι αρχές QPUF μπορούν να εφαρμοστούν και σε οικιακές συσκευές για την εξασφάλιση μοναδικής ταυτότητας και την αποτροπή κλωνοποίησης ή παραποίησης hardware.

Παράλληλα, οι Elmarkez et al. (2025) εξετάζουν το secure-by-design από την οπτική των industrial control systems, παρουσιάζοντας ένα systematic mapping study που δείχνει πως η ενσωμάτωση ασφαλείας στο επίπεδο της αρχιτεκτονικής μπορεί να μειώσει δραστικά τον κίνδυνο επιθέσεων σε cyber–physical περιβάλλοντα. Αν και οι μελέτες τους εστιάζουν στο ICS, οι αρχές που απορρέουν—όπως modular security layering, predictive threat analysis και continuous validation—έχουν άμεση εφαρμογή σε smart home υποδομές, όπου οι συσκευές πρέπει να διαχειρίζονται πολλαπλές πηγές δεδομένων και δυναμικές συνδέσεις.

Η εφαρμογή secure-by-design σε πραγματικά περιβάλλοντα αποτυπώνεται και στο έργο των Marchang et al. (2024), οι οποίοι παρουσιάζουν μια real-time IoMT

αρχιτεκτονική ασφαλείας για πληθυσμιακή υγειονομική παρακολούθηση. Η μελέτη τους προτείνει ένα πολυεπίπεδο πλαίσιο προστασίας, το οποίο ενσωματώνει cryptographic safeguards, policy enforcement modules και mechanisms for continuous threat assessment. Τα συστατικά αυτά μπορούν να προσαρμοστούν σε περιβάλλοντα smart home που υποστηρίζουν συσκευές υγείας, όπως smart medical sensors.

Ιστορικά, το secure-by-design έχει τις ρίζες του σε middleware frameworks όπως το S-MARKS των Ahamed et al. (2007), το οποίο αποτελεί ένα από τα πρώτα παραδείγματα ενσωμάτωσης ασφάλειας από τα κατώτερα στρώματα του λογισμικού. Η αρχιτεκτονική S-MARKS δείχνει ότι η ασφαλής δομή ενός συστήματος μπορεί να διασφαλιστεί ήδη από το επίπεδο της middleware υποδομής, κάτι που αποτελεί σημαντικό δίδαγμα για τη σύγχρονη σχεδίαση IoT πλατφορμών, όπου η ασφάλεια πρέπει να ενσωματώνεται από τα foundational layers.

Η εφαρμογή privacy-by-design επηρεάζεται επίσης από τις απαιτήσεις cloud-native αρχιτεκτονικών. Σύμφωνα με τον Varri (2021), η ασφαλής σχεδίαση για υβριδικές cloud υποδομές απαιτεί ενσωματωμένα access control policies, segmentation, encryption-at-rest/encryption-in-transit και συνεχή αξιολόγηση κινδύνου. Τα smart homes χρησιμοποιούν σε μεγάλο βαθμό cloud υπηρεσίες για λειτουργίες αυτοματισμού, γεγονός που σημαίνει ότι οι αρχές cloud-native security πρέπει να εφαρμόζονται ολιστικά.

Η βιβλιογραφία αποδεικνύει ότι η ενσωμάτωση secure-by-design και privacy-by-design αρχών είναι απαραίτητη για τη δημιουργία ανθεκτικών smart home συστημάτων. Τα βασικά στοιχεία αυτών των αρχιτεκτονικών περιλαμβάνουν:

- Ανάλυση κινδύνου από το στάδιο σχεδιασμού μέσω συστηματικών μοντέλων απειλών.
- Ελαχιστοποίηση δεδομένων και προστασία ιδιωτικότητας μέσω περιορισμένης συλλογής και τοπικής επεξεργασίας.
- Ενσωμάτωση κρυπτογραφίας και μηχανισμών ελέγχου πρόσβασης στα πρώτα στάδια της υλοποίησης.
- Συμμόρφωση με κανονιστικά πλαίσια όπως GDPR, NIS2 και ISO/IEC 27001.

- Διαρκής επικαιροποίηση και adaptive security models, ώστε τα συστήματα να προσαρμόζονται σε νέες απειλές.

Η υιοθέτηση αυτών των προσεγγίσεων αποτελεί βασική προϋπόθεση για την αξιόπιστη και ασφαλή λειτουργία των έξυπνων σπιτιών, ενώ ταυτόχρονα ενισχύει την εμπιστοσύνη των χρηστών και την ανθεκτικότητα του οικοσυστήματος απέναντι σε κυβερνοεπιθέσεις.

3.3 Μελέτες σχετικά με την ιδιωτικότητα και τη συμπεριφορά χρηστών

Πέρα από τις καθαρά τεχνικές προσεγγίσεις, ένα σημαντικό κομμάτι της βιβλιογραφίας εστιάζει στο πώς οι ίδιοι οι χρήστες αντιλαμβάνονται την ασφάλεια και την ιδιωτικότητα στα έξυπνα σπίτια, πώς χρησιμοποιούν τις συσκευές και πώς οι κοινωνικές σχέσεις μέσα στο σπίτι αλληλεπιδρούν με τις τεχνικές δυνατότητες του συστήματος.

Οι πρώτες συστηματικές ποιοτικές μελέτες, όπως αυτή των Jacobsson και Davidsson, δείχνουν ότι οι ένοικοι συχνά υποτιμούν τους κινδύνους που συνδέονται με τη διασύνδεση των οικιακών συσκευών στο διαδίκτυο, ενώ βασίζονται σε ad hoc πρακτικές, όπως η αλλαγή ενός μόνο password ή η αποφυγή ορισμένων λειτουργιών, χωρίς συνολική κατανόηση του συστήματος (Jacobsson & Davidsson, 2015). Η ίδια μελέτη υπογραμμίζει ότι αρκετοί χρήστες θεωρούν ως «καθαρά τεχνικό» ζήτημα την ασφάλεια, αναμένοντας ότι ο πάροχος υπηρεσιών ή ο κατασκευαστής έχει ήδη λάβει όλα τα απαραίτητα μέτρα.

Ένα σημαντικό βήμα προς την κατανόηση των ανησυχιών των τελικών χρηστών πραγματοποιούν οι Zeng et al., οι οποίοι διεξήγαγαν ημι-δομημένες συνεντεύξεις με δεκαπέντε άτομα που ζουν σε έξυπνα σπίτια, εκ των οποίων δώδεκα ήταν διαχειριστές του συστήματος και τρεις απλοί χρήστες (Zeng et al., 2017) Τα ευρήματά τους δείχνουν, μεταξύ άλλων, ότι οι χρήστες έχουν περιορισμένη τεχνική κατανόηση του πώς λειτουργούν οι συσκευές και οι πλατφόρμες, με αποτέλεσμα το νοητικό τους μοντέλο για τις απειλές να είναι αποσπασματικό. Παρότι οι περισσότεροι συμμετέχοντες είχαν ακούσει για επιθέσεις όπως το Mirai, δεν αισθάνονταν ιδιαίτερα

ευάλωτοι, είτε λόγω ελλιπούς κατανόησης είτε λόγω μιας μορφής «κόπωσης» απέναντι στην πληθώρα ειδήσεων για κυβερνοεπιθέσεις.

Σε μεταγενέστερη εργασία, οι Zeng και Roesner εξετάζουν ειδικά τα ζητήματα που ανακύπτουν σε πολυχρηστικά έξυπνα σπίτια. Μέσα από μια μελέτη διάρκειας ενός μήνα σε επτά νοικοκυριά, με συνολικό αριθμό δεκαεννέα συμμετεχόντων, οι συγγραφείς ανέλυσαν πώς οι χρήστες αλληλεπιδρούν με προηγμένες λειτουργίες ελέγχου πρόσβασης, όπως κανόνες βάσει τοποθεσίας και εποπτικοί λογαριασμοί. Ένα από τα βασικά ευρήματα είναι ότι, παρόλο που οι συμμετέχοντες αναγνώρισαν θεωρητικά πολλές περιπτώσεις όπου θα ήθελαν πιο ευέλικτο έλεγχο πρόσβασης (π.χ. για νταντάδες, φιλοξενούμενους ή παιδιά), στην πράξη ελάχιστοι αξιοποίησαν τις αντίστοιχες λειτουργίες. Οι λόγοι περιλαμβάνουν την πολυπλοκότητα των διεπαφών, το γεγονός ότι οι χρήστες θεωρούσαν «αρκετή» τη ρύθμιση μέσω κοινωνικών κανόνων και εμπιστοσύνης, αλλά και την ανησυχία ότι ο υπερβολικά αυστηρός έλεγχος θα δυσχέραινε τη χρήση (Zeng & Roesner, 2019)

Η σημασία των κοινωνικών και εξουσιαστικών σχέσεων μέσα στο νοικοκυριό υπογραμμίζεται επίσης στη βιβλιογραφία που συνοψίζεται από τους Kraemer και Flechais. Οι συγγραφείς τονίζουν ότι τα smart homes συχνά ενισχύουν ήδη υπάρχουσες ανισορροπίες ισχύος, καθώς ο «τεχνολογικά ικανός» χρήστης που εγκαθιστά και ρυθμίζει τις συσκευές αποκτά αυξημένο έλεγχο πάνω στο περιβάλλον και στα δεδομένα των υπόλοιπων ενοίκων (Kraemer & Flechais, 2018). Αυτό μπορεί να οδηγήσει σε διακριτικές μορφές επιτήρησης ή περιορισμού, οι οποίες γίνονται δύσκολα αντιληπτές από τα υπόλοιπα μέλη, ειδικά όταν πρόκειται για παιδιά ή ηλικιωμένους.

Στο ίδιο πνεύμα, ο Renu παραθέτει στατιστικά στοιχεία για την κλίμακα των παραβιάσεων δεδομένων, αναφέροντας ότι το 2019 παραβιάστηκαν πάνω από δύο δισεκατομμύρια αρχεία πελατών, σύμφωνα με αναφορές μεγάλων οργανισμών (Renu, 2019). Παρότι τα στοιχεία αυτά δεν αφορούν αποκλειστικά έξυπνα σπίτια, δείχνουν ότι οι χρήστες λειτουργούν σε ένα περιβάλλον όπου οι παραβιάσεις είναι συχνές και μεγάλης κλίμακας, γεγονός που επηρεάζει τις αντιλήψεις τους για την αναπόφευκτη, σχεδόν «κανονικοποιημένη» φύση των κινδύνων.

Νεότερες εργασίες, όπως αυτή των Harvey et al. για τις ιατρικές συσκευές σε smart homes, αναδεικνύουν επιπλέον την ανάγκη για ευαισθητοποίηση των χρηστών γύρω

από τις συνέπειες της διαρροής ιατρικών δεδομένων. Οι συγγραφείς επισημαίνουν ότι οι χρήστες σπάνια αντιλαμβάνονται ότι πληροφορίες όπως η συχνότητα χρήσης μιας συσκευής εισπνοών ή οι ώρες παρακολούθησης συγκεκριμένων βιοσημάτων μπορούν να αποκαλύψουν λεπτομέρειες για τη καθημερινή ρουτίνα, τις ώρες απουσίας από το σπίτι ή ακόμα και τη συμμόρφωση σε θεραπευτικά σχήματα (Harvey et al., 2020).

Ιδιαίτερο ενδιαφέρον παρουσιάζουν και οι μελέτες που εξετάζουν όχι μόνο τους ενοίκους, αλλά και τους «παριστάμενους» (bystanders), όπως επισκέπτες ή εργαζόμενους στο σπίτι. Οι εργασίες που συνοψίζονται από τους Albayaydh et al. δείχνουν ότι οι παριστάμενοι συχνά δεν γνωρίζουν την ύπαρξη συσκευών καταγραφής (π.χ. καμερών και μικροφώνων), ενώ όταν ενημερώνονται, εκφράζουν ανησυχίες για την πιθανή χρήση των δεδομένων σε μελλοντικές αξιολογήσεις ή συγκρούσεις. Η διάσταση αυτή της ιδιωτικότητας είναι ιδιαίτερα σημαντική σε χώρους όπως Airbnb ή σπίτια με οικιακό προσωπικό, όπου τα όρια ανάμεσα σε ιδιωτικό και επαγγελματικό χώρο θολώνουν.

Τέλος, η εργασία των Albayaydh et al. (2025) επιχειρεί να συνδέσει τις παραπάνω παρατηρήσεις με τον ρόλο των συστημάτων τεχνητής νοημοσύνης, προτείνοντας ότι έξυπνοι βοηθοί μπορούν να λειτουργήσουν ως «διαμεσολαβητές» ιδιωτικότητας. Σύμφωνα με τα ευρήματά τους, εργαλεία βασισμένα σε γενετική ΤΝ μπορούν να βοηθήσουν χρήστες με περιορισμένη τεχνική κατάρτιση να κατανοήσουν καλύτερα τις επιπτώσεις των ρυθμίσεων ιδιωτικότητας και να λάβουν πιο ενημερωμένες αποφάσεις, υπό την προϋπόθεση ότι οι ίδιες οι πλατφόρμες τηρούν υψηλά πρότυπα διαφάνειας και λογοδοσίας.

Οι μελέτες για την ιδιωτικότητα και τη συμπεριφορά των χρηστών στα έξυπνα σπίτια καταδεικνύουν μια σταθερή τάση: οι τεχνικές δυνατότητες των συστημάτων ασφάλειας και ιδιωτικότητας συχνά υπερβαίνουν την πραγματική ικανότητα και διάθεση των χρηστών να τις κατανοήσουν και να τις αξιοποιήσουν. Η ύπαρξη σύνθετων μηχανισμών ελέγχου πρόσβασης, διαχείρισης δικαιωμάτων και ορατότητας δεν εγγυάται από μόνη της προστασία, εάν οι διεπαφές είναι δυσνόητες, εάν οι κοινωνικές σχέσεις εντός του σπιτιού δημιουργούν ανισορροπίες ισχύος ή εάν οι χρήστες έχουν συμβιβαστεί με την ιδέα ότι η πλήρης ιδιωτικότητα είναι ανέφικτη.

Η βιβλιογραφική ανασκόπηση δείχνει, επομένως, ότι οποιαδήποτε ουσιαστική προσέγγιση στην ασφάλεια και την ιδιωτικότητα στα smart homes οφείλει να συνδυάζει τεχνικές λύσεις με ανθρωποκεντρικό σχεδιασμό και κατανόηση των κοινωνικών δυναμικών του οικιακού περιβάλλοντος.

3.3.1. Αντίληψη των χρηστών για την ιδιωτικότητα σε έξυπνα σπίτια

Η αντίληψη των χρηστών σχετικά με την ιδιωτικότητα στα έξυπνα σπίτια αποτελεί θεμελιώδη παράμετρο για την αξιολόγηση της αποδοχής και της βιώσιμης χρήσης των IoT τεχνολογιών. Η συνεχής συλλογή δεδομένων από αισθητήρες, κάμερες, φωνητικούς βοηθούς και συσκευές καθημερινής χρήσης δημιουργεί ένα περιβάλλον υψηλής διαφάνειας, το οποίο συχνά έρχεται σε αντίθεση με τις προσδοκίες των χρηστών για έλεγχο, ασφάλεια και περιορισμένη παρακολούθηση. Η βιβλιογραφία αναδεικνύει ότι η αντίληψη της ιδιωτικότητας είναι πολυδιάστατη και επηρεάζεται από παράγοντες όπως η εμπιστοσύνη προς τις εταιρείες, το επίπεδο τεχνογνωσίας, η εξοικείωση με την τεχνολογία, οι πολιτισμικές παράμετροι και τα ατομικά χαρακτηριστικά των χρηστών.

Ένα από τα πρώτα συστηματικά ευρήματα προέρχεται από τους Schomakers et al. (2021), οι οποίοι αναλύουν τις προτιμήσεις των χρηστών σε σχέση με την αυτοματοποίηση των έξυπνων σπιτιών και καταγράφουν ότι η ιδιωτικότητα και η εμπιστοσύνη αποτελούν δύο από τους σημαντικότερους παράγοντες που καθορίζουν την πρόθεση υιοθέτησης. Οι χρήστες θεωρούν ιδιαίτερα ευαίσθητες τις πληροφορίες που αφορούν συνήθειες, μοτίβα παρουσίας-απουσίας, βιντεοληπτικά δεδομένα και ηχητικές καταγραφές. Ιδίως οι φωνητικοί βοηθοί αντιμετωπίζονται με επιφυλακτικότητα λόγω της συνεχούς ενεργοποίησης των μικροφώνων, η οποία δημιουργεί την αίσθηση μη ελεγχόμενης παρακολούθησης.

Έρευνα των Zheng et al. (2018) αποκαλύπτει ότι οι περισσότεροι χρήστες δεν έχουν σαφή εικόνα για το τι δεδομένα συλλέγουν οι συσκευές τους, πού αποθηκεύονται και με ποιους διαμοιράζονται. Η έλλειψη διαφάνειας στις πολιτικές απορρήτου οδηγεί σε χαμηλή εμπιστοσύνη προς τους κατασκευαστές, ενώ οι ανησυχίες εντείνονται όταν τα δεδομένα μεταφέρονται σε τρίτους παρόχους μέσω cloud υπηρεσιών. Οι συγγραφείς υπογραμμίζουν ότι ακόμη και χρήστες με υψηλή τεχνογνωσία συχνά αδυνατούν να

αποτιμήσουν τους πραγματικούς κινδύνους, καθώς οι IoT οικοσυστήματα χαρακτηρίζονται από πολυπλοκότητα και αδιαφάνεια.

Συμπληρωματικά, οι Schomakers et al. (2020) δείχνουν ότι η εμπιστοσύνη δεν αφορά μόνο την τεχνική ασφάλεια, αλλά και την αξιοπιστία και τις προθέσεις των παρόχων υπηρεσιών. Οι χρήστες παρουσιάζουν υψηλότερη ανοχή σε τεχνολογικούς κινδύνους όταν θεωρούν ότι ο πάροχος ενεργεί με υπευθυνότητα και προστατεύει τα συμφέροντά τους. Αντίθετα, ακόμη και μικρές παραβιάσεις ή ασαφείς πολιτικές χρήσης δεδομένων μπορεί να οδηγήσουν σε σημαντική μείωση εμπιστοσύνης.

Το θέμα των δημογραφικών διαφορών αναδεικνύεται ιδιαίτερα από τη μελέτη των Singh et al. (2018), οι οποίοι εξετάζουν πώς διαφορετικές ηλικιακές ομάδες και επίπεδα τεχνολογικής εξοικείωσης επηρεάζουν την αποδοχή των έξυπνων συσκευών. Οι νεότεροι χρήστες εμφανίζονται περισσότερο δεκτικοί, αλλά όχι απαραίτητα λιγότερο ανήσυχοι· αντιθέτως, τείνουν να γνωρίζουν καλύτερα τις πιθανές απειλές και απαιτούν μηχανισμούς ελέγχου και διαφάνειας. Οι μεγαλύτεροι σε ηλικία χρήστες υιοθετούν την τεχνολογία πιο επιφυλακτικά, συνήθως λόγω έλλειψης κατανόησης των λειτουργιών και των πρωτοκόλλων που διέπουν την επεξεργασία δεδομένων.

Εξίσου σημαντική είναι και η οπτική των τρίτων —επισκεπτών ή μελών της οικογένειας— όπως αναλύεται από τους Yao et al. (2019). Τα ευρήματα δείχνουν ότι οι παρευρισκόμενοι σε ένα έξυπνο σπίτι συχνά δεν αισθάνονται ότι έχουν τον ίδιο βαθμό ελέγχου με τον ιδιοκτήτη, με αποτέλεσμα να θεωρούν ορισμένες τεχνολογίες παρεμβατικές ή ακόμη και ανεπιθύμητες. Οι ανησυχίες τους επικεντρώνονται κυρίως σε κάμερες, μικρόφωνα και συσκευές που συλλέγουν βιομετρικά δεδομένα, όπου ένα σημαντικό ποσοστό χρηστών θεωρεί ότι παραβιάζεται η προσωπική τους σφαίρα χωρίς τη συναίνεσή τους.

Η εμπιστοσύνη προς τις συσκευές αποτελεί επίσης καθοριστικό παράγοντα, όπως δείχνει η εργασία των Liu et al. (2021), η οποία επικεντρώνεται σε φωνητικά συστήματα έξυπνων σπιτιών. Οι χρήστες τείνουν να εμπιστεύονται περισσότερο συσκευές που παρέχουν μηχανισμούς οπτικής ή ηχητικής ένδειξης όταν γίνεται συλλογή δεδομένων. Επιπλέον, η σαφής ενημέρωση για το πότε ενεργοποιείται η καταγραφή ή πού αποθηκεύονται τα δεδομένα ενισχύει σημαντικά το επίπεδο αντιληπτής ασφάλειας.

Από διαφορετική σκοπιά, οι Kennedy et al. (2021) εστιάζουν στην αντίληψη των χρηστών σε πλαίσια έρευνας, όπου ζητείται εγκατάσταση IoT συσκευών για τη μελέτη της καθημερινότητας. Οι συμμετέχοντες περιγράφουν την εμπιστοσύνη ως «άλμα πίστης», τονίζοντας ότι παρόλο που αναγνωρίζουν τους κινδύνους, επιλέγουν να προχωρήσουν μόνο όταν η έρευνα ή ο πάροχος θεωρείται αξιόπιστος. Μεταφέρουν μάλιστα ότι η συναίνεση δεν είναι απλώς διαδικαστική, αλλά συνδέεται με συναισθηματικούς παράγοντες, όπως η αίσθηση ελέγχου και η σχέση με τον φορέα εγκατάστασης.

Οι Magara & Zhou (2024) πραγματοποιούν μια ολοκληρωμένη user-centric ανάλυση και επισημαίνουν ότι η αντίληψη κινδύνου επηρεάζει άμεσα την πρόθεση υιοθέτησης της τεχνολογίας. Οι χρήστες που θεωρούν τα IoT συστήματα ευάλωτα σε κυβερνοεπιθέσεις είναι λιγότερο πιθανό να τα εγκαταστήσουν, ενώ όσοι έχουν εξοικείωση με την τεχνολογία εμφανίζουν μεγαλύτερη εμπιστοσύνη, όχι απαραίτητα επειδή αξιολογούν διαφορετικά τον κίνδυνο, αλλά λόγω αυξημένης ικανότητας διαχείρισης των ρυθμίσεων απορρήτου.

Σημαντική συμβολή στη συζήτηση προσφέρουν οι Guhr et al. (2020), οι οποίοι δείχνουν ότι οι ανησυχίες των χρηστών συχνά σχετίζονται με την αβεβαιότητα ως προς τον τρόπο αξιοποίησης των δεδομένων. Η αίσθηση ότι τα δεδομένα «θα μπορούσαν» να χρησιμοποιηθούν εναντίον τους (π.χ. profiling, στοχευμένες διαφημίσεις, παρακολούθηση συμπεριφοράς) ενισχύει την ψυχολογική αντίσταση απέναντι στην τεχνολογία. Οι συγγραφείς επισημαίνουν ότι οι χρήστες τείνουν να υπερεκτιμούν ορισμένους κινδύνους και να υποτιμούν άλλους, ειδικά όταν δεν διαθέτουν τεχνική γνώση.

Από κοινωνιοτεχνική προοπτική, οι Grünewald & Reisch (2020) εξετάζουν τη χρήση δεδομένων για ενεργειακές υπηρεσίες στο Ηνωμένο Βασίλειο και εντοπίζουν σημαντική «ψαλίδα εμπιστοσύνης» (trust gap). Οι πολίτες εμφανίζονται διατεθειμένοι να παρέχουν δεδομένα μόνο όταν έχουν σαφή εικόνα του οφέλους. Αν το όφελος δεν είναι άμεσα ορατό ή δεν εξηγείται επαρκώς, η αντίληψη κινδύνου αυξάνεται, με αποτέλεσμα τη χαμηλή αποδοχή.

Ενδιαφέροντα ευρήματα προκύπτουν επίσης από τη μελέτη των Alraja et al. (2019), οι οποίοι αναλύουν τη σχέση ιδιωτικότητας, ασφάλειας και ρίσκου σε IoT συστήματα

υγείας. Αν και το αντικείμενο αφορά τον τομέα της υγείας, πολλά στοιχεία μεταφέρονται αυτούσια στα έξυπνα σπίτια· οι χρήστες παρουσιάζουν υψηλή ανησυχία για την αποκάλυψη ευαίσθητων δεδομένων, αλλά ταυτόχρονα επιθυμούν την ευκολία που προσφέρει η τεχνολογία. Η αντίληψη ρίσκου λειτουργεί ως ενδιάμεσος παράγοντας που καθορίζει σε ποιο βαθμό η εμπιστοσύνη και η εξοικείωση μετατρέπονται σε θετική στάση προς τις συσκευές.

Τέλος, οι Li et al. (2023) παρουσιάζουν εντυπωσιακά ευρήματα από χρήστες του Reddit, δείχνοντας ότι πολλοί θεωρούν πως η προστασία της ιδιωτικότητας αποτελεί αποκλειστική ευθύνη του καταναλωτή. Αυτή η αντίληψη οδηγεί σε υψηλή ανοχή κινδύνου και συχνά σε κακή διαχείριση των ρυθμίσεων ασφαλείας, ενώ παράλληλα αναδεικνύει την ανάγκη για πιο υπεύθυνο σχεδιασμό συσκευών και σαφέστερη επικοινωνία από τους κατασκευαστές.

Η βιβλιογραφία καταδεικνύει ότι η αντίληψη της ιδιωτικότητας στα έξυπνα σπίτια είναι σύνθετη και πολυδιάστατη. Οι χρήστες επιθυμούν έλεγχο, διαφάνεια και σαφή ενημέρωση, ενώ οι δημογραφικές και γνωστικές διαφορές επηρεάζουν σημαντικά την εμπιστοσύνη, την ανησυχία και την πρόθεση υιοθέτησης. Η κατανόηση αυτών των παραγόντων είναι κρίσιμη για τον σχεδιασμό αποτελεσματικών, κοινωνικά αποδεκτών και ηθικά τεκμηριωμένων τεχνολογιών έξυπνων σπιτιών.

3.3.2. Παράγοντες που επηρεάζουν την υιοθέτηση ή την απόρριψη smart home συστημάτων

Η υιοθέτηση των smart home συστημάτων αποτελεί αντικείμενο εκτενούς έρευνας τα τελευταία χρόνια, με πλήθος μελετών να αξιοποιούν καθιερωμένα μοντέλα αποδοχής τεχνολογίας όπως το Technology Acceptance Model (TAM), το Unified Theory of Acceptance and Use of Technology (UTAUT και UTAUT2), το Theory of Planned Behavior (TPB), καθώς και διάφορες επεκτάσεις των μοντέλων αυτών. Τα μοντέλα αυτά προσφέρουν ένα θεωρητικό πλαίσιο για την κατανόηση των παραγόντων που επηρεάζουν θετικά ή αρνητικά την πρόθεση χρήσης smart home τεχνολογιών, λαμβάνοντας υπόψη τόσο τις τεχνικές πτυχές όσο και τις ψυχολογικές, κοινωνικές και δημογραφικές διαστάσεις.

Στη συστηματική ανασκόπησή τους, οι Mashal et al. (2023) εξετάζουν δέκα χρόνια έρευνας για την υιοθέτηση smart home τεχνολογιών και διαπιστώνουν ότι οι πιο συχνά αναφερόμενοι παράγοντες είναι η αντιληπτή χρησιμότητα (perceived usefulness), η ευκολία χρήσης (perceived ease of use), η εμπιστοσύνη, η ασφάλεια, το απόρρητο, η σχέση κόστους–οφέλους και η αξιοπιστία των συσκευών. Τα συμπεράσματα της ανασκόπησης υποστηρίζουν ότι οι χρήστες υιοθετούν smart home συστήματα όταν διαπιστώνουν σαφή οφέλη που υπερτερούν των αντιλαμβανόμενων κινδύνων, ενώ η εποικοδομητική επικοινωνία με τους παρόχους ενισχύει την αποδοχή.

Αντίστοιχα, οι Salimon et al. (2018) προτείνουν ένα ολοκληρωμένο μοντέλο που συνδυάζει TAM3, TPB και UTAUT2 προκειμένου να προβλέψουν με μεγαλύτερη ακρίβεια την υιοθέτηση smart home τεχνολογιών στη Μαλαισία. Η μελέτη τονίζει τη σημασία κοινωνικών επιρροών (social influence), της αντιληπτής ευκολίας χρήσης, της παρακινητικής συμπεριφοράς, αλλά και της συμβατότητας (compatibility) της τεχνολογίας με τις καθημερινές συνήθειες των χρηστών. Το οικονομικό κόστος εμφανίζεται ως σημαντικός ανασταλτικός παράγοντας, ειδικά σε αναδυόμενες αγορές, όπου οι χρήστες θεωρούν τα smart home συστήματα ως είδος πολυτελείας.

Η έρευνα των Shuhaiber & Mashal (2019) τονίζει ότι η εμπιστοσύνη (trust) αποτελεί κρίσιμο παράγοντα στην αποδοχή των smart home συστημάτων. Οι χρήστες τείνουν να απορρίπτουν τεχνολογίες που θεωρούν περίπλοκες, δύσκολες στη διαχείριση ή επικίνδυνες για την ασφάλεια και το απόρρητό τους. Το TAM μοντέλο επιβεβαιώνεται ως ιδιαίτερα αποτελεσματικό στη μέτρηση της πρόθεσης χρήσης, ωστόσο οι συγγραφείς προσθέτουν επιπλέον μεταβλητές όπως perceived control και perceived risk για να ενισχύσουν την ερμηνευτική ικανότητα του μοντέλου.

Εστιάζοντας σε συγκεκριμένες πληθυσμιακές ομάδες, οι Zhou et al. (2024) εξετάζουν την πρόθεση χρήσης smart home τεχνολογιών από ηλικιωμένους καταναλωτές, αναδεικνύοντας παράγοντες όπως η αντιληπτή αξιοπιστία, η ανάγκη για υποστήριξη της καθημερινότητας και η ευκολία στην εκμάθηση. Η κοινωνική επιρροή και η προηγούμενη εμπειρία με ψηφιακές τεχνολογίες παίζουν καθοριστικό ρόλο, καθώς οι ηλικιωμένοι χρήστες εμφανίζουν συχνά χαμηλότερο επίπεδο αυτο-αποτελεσματικότητας (self-efficacy) και μεγαλύτερη ανάγκη για υποστήριξη και καθοδήγηση.

Συμπληρωματικά, οι Pal et al. (2018) επιβεβαιώνουν ότι η τεχνολογία smart home μπορεί να συμβάλει σημαντικά στην ανεξαρτησία των ηλικιωμένων, ωστόσο η υιοθέτηση παραμένει περιορισμένη λόγω φόβων σχετικά με την ιδιωτικότητα, την υποκλοπή δεδομένων και τη δυσκολία χρήσης. Το UTAUT μοντέλο αποδεικνύεται ιδιαίτερα αποτελεσματικό, καθώς συμπεριλαμβάνει παράγοντες όπως η προσδοκώμενη προσπάθεια (effort expectancy) και η ευκολία πρόσβασης σε υποστήριξη (facilitating conditions).

Σε αντίστοιχο πλαίσιο, η έρευνα των Arar et al. (2021) δείχνει ότι οι ηλικιωμένοι χρήστες στο Ντουμπάι αντιλαμβάνονται τα smart home συστήματα ως ιδιαίτερα χρήσιμα για την αύξηση της άνεσης και της ασφάλειας. Ωστόσο, η τεχνολογική ανησυχία (technology anxiety) και η αντίληψη περί πολυπλοκότητας μπορούν να μειώσουν την πρόθεση χρήσης. Η μελέτη επιβεβαιώνει ότι η αποτελεσματική σχεδίαση διεπαφών και η απλοποίηση των λειτουργιών είναι κεντρικές προϋποθέσεις για την υιοθέτηση.

Η αποδοχή των smart home συστημάτων δεν περιορίζεται σε γενικές συσκευές, αλλά εκτείνεται και σε εξειδικευμένες εφαρμογές όπως οι smart locks. Οι Mamonov & Benbunan-Fich (2021) δείχνουν ότι οι χρήστες εστιάζουν στην αντιληπτή ασφάλεια, την αξιοπιστία και την ευκολία χρήσης. Τα smart locks αντιμετωπίζονται συχνά με καχυποψία λόγω πιθανών τεχνικών δυσλειτουργιών ή φόβων για κυβερνοεπιθέσεις. Ωστόσο, η προσδοκώμενη απόδοση (performance expectancy) και η ευκολία ενσωμάτωσης στην καθημερινότητα ενισχύουν την πρόθεση υιοθέτησης.

Η έρευνα σε νεότερους χρήστες, όπως αυτή του Choi (2023), επιβεβαιώνει ότι το TAM παραμένει ιδιαίτερα αποτελεσματικό στην πρόβλεψη αποδοχής των smart homes από φοιτητές. Η αντιληπτή χρησιμότητα είναι ο ισχυρότερος προβλεπτικός παράγοντας, ενώ η αντιληπτή ευκολία χρήσης λειτουργεί ως έμμεσος ενισχυτής. Οι φοιτητές είναι πιο πρόθυμοι να υιοθετήσουν τεχνολογίες που συμβάλλουν στην εξοικονόμηση χρόνου και στην αύξηση της άνεσης.

Οι Cimperman et al. (2016) εξετάζουν επίσης την εφαρμογή ενός επεκταμένου μοντέλου UTAUT σε υπηρεσίες τηλεϊατρικής για ηλικιωμένους, και παρόλο που το περιβάλλον δεν αφορά αυστηρά smart homes, τα ευρήματα έχουν άμεση συνάφεια. Διαπιστώνεται ότι η αντιληπτή αξία και η κοινωνική επιρροή είναι ιδιαίτερα

σημαντικοί παράγοντες για την πρόθεση χρήσης νέων τεχνολογιών από ευάλωτες πληθυσμιακές ομάδες.

Σε πιο πρόσφατη ανασκόπηση, οι Valencia-Arias et al. (2023) συγκεντρώνουν τα κυριότερα ευρήματα της διεθνούς βιβλιογραφίας και προτείνουν ένα ενοποιημένο ερευνητικό πλαίσιο. Η μελέτη δείχνει ότι οι αρνητικοί παράγοντες υιοθέτησης περιλαμβάνουν τον φόβο παραβίασης δεδομένων, το οικονομικό κόστος, την τεχνολογική πολυπλοκότητα και την αντιληπτή έλλειψη αξιοπιστίας. Οι θετικοί παράγοντες περιλαμβάνουν την άνεση, την ασφάλεια, την εξοικονόμηση ενέργειας και την ενίσχυση της ποιότητας ζωής.

Τέλος, η εργασία της Lilian (2024) επιβεβαιώνει εκ νέου ότι το TAM αποτελεί αξιόπιστο μοντέλο πρόβλεψης της υιοθέτησης smart home συστημάτων, αναδεικνύοντας τη σημαντική επίδραση της αντιληπτής χρησιμότητας και της ευκολίας χρήσης. Η συγγραφέας τονίζει ότι οι χρήστες προσεγγίζουν τα smart homes μέσα από το πρίσμα του λειτουργικού οφέλους σε σχέση με την ιδιωτικότητα, κάτι που υποδεικνύει μια συνεχή ανάγκη για σχεδιασμό ασφαλών και εύχρηστων συστημάτων.

Η βιβλιογραφία δείχνει ότι οι βασικοί παράγοντες που επηρεάζουν την υιοθέτηση smart home τεχνολογιών είναι:

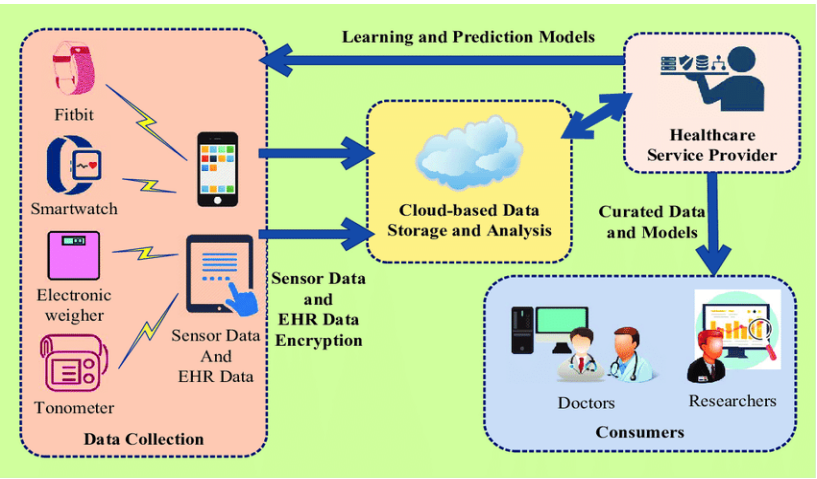
- Αντιληπτή χρησιμότητα – η επίδραση στην άνεση, ασφάλεια και αποτελεσματικότητα.
- Ευκολία χρήσης – η απλότητα εγκατάστασης και λειτουργίας.
- Ασφάλεια και ιδιωτικότητα – φόβοι παραβίασης δεδομένων και κυβερνοεπιθέσεων.
- Κόστος – τόσο οικονομικό όσο και λειτουργικό.
- Εμπιστοσύνη στους παρόχους – αξιοπιστία, διαφάνεια, υποστήριξη.
- Κοινωνική επιρροή – επιρροές από οικογένεια, φίλους και επαγγελματικές γνωριμίες.
- Δημογραφικές διαφοροποιήσεις – ηλικία, τεχνογνωσία, προσωπικές ανάγκες.

Η κατανόηση των παραγόντων αυτών αποτελεί κρίσιμη προϋπόθεση για το σχεδιασμό τεχνολογιών που θα γίνουν κοινωνικά αποδεκτές και πραγματικά χρήσιμες για τους κατοίκους ενός έξυπνου σπιτιού.

3.3.3. Κίνδυνοι διαρροής δεδομένων και θέματα profiling

Η εκτεταμένη χρήση έξυπνων συσκευών στα smart homes έχει ως αποτέλεσμα τη συνεχή συλλογή δεδομένων που αφορούν τις καθημερινές δραστηριότητες των χρηστών. Τα δεδομένα αυτά, τα οποία προέρχονται από αισθητήρες κίνησης, έξυπνους μετρητές ενέργειας, κάμερες, Wi-Fi routers, φωνητικούς βοηθούς και αυτοματισμούς, μπορούν να αποκαλύψουν λεπτομερή μοτίβα συμπεριφοράς. Η βιβλιογραφία καταδεικνύει ότι ακόμη και αν τα δεδομένα δεν περιλαμβάνουν απευθείας προσωπικά αναγνωρίσιμες πληροφορίες, η επαναλαμβανόμενη ανάλυση της χρήσης συσκευών μπορεί να οδηγήσει σε ακριβή profiling των χρηστών, εγείροντας σημαντικούς κινδύνους για την ιδιωτικότητα.

Στην Εικόνα 7 απεικονίζεται ένα σενάριο συλλογής και επεξεργασίας δεδομένων υγείας μέσω συσκευών IoT, όπου αισθητήρες και φορετές συσκευές αποστέλλουν κρυπτογραφημένα δεδομένα σε υποδομές cloud για ανάλυση και πρόβλεψη. Η αρχιτεκτονική αυτή αναδεικνύει κρίσιμα ζητήματα ιδιωτικότητας, καθώς η συγκέντρωση και διαμοίραση δεδομένων σε παρόχους υπηρεσιών υγείας και τρίτους φορείς αυξάνει τον κίνδυνο profiling, μη εξουσιοδοτημένης πρόσβασης και απώλειας ελέγχου από τον χρήστη.



Εικόνα 7. Ροή δεδομένων IoT υγείας και επεξεργασία μέσω cloud υποδομών με έμφαση στην ασφάλεια και την ιδιωτικότητα. Πηγή: (Haris et al., 2023)

Οι Park et al. (2014) αναδεικνύουν ότι η κατανάλωση ενέργειας αποτελεί ένα από τα πιο χαρακτηριστικά παραδείγματα ακούσιας διαρροής δεδομένων. Μέσα από την ανάλυση των ενεργειακών προτύπων μπορούν να εξαχθούν πληροφορίες για το πότε οι χρήστες είναι στο σπίτι, ποιες συσκευές χρησιμοποιούν, ακόμη και λεπτομέρειες σχετικά με τον τρόπο ζωής τους. Στη μελέτη τους προτείνεται η χρήση privacy-preserving τεχνικών που αποσκοπούν στην απόκρυψη σημασιολογικών πληροφοριών μέσω ενεργειακής εξομάλυνσης, γεγονός που αποδεικνύει πόσο στενά συνδέονται τα λειτουργικά δεδομένα με την ιδιωτικότητα.

Εξίσου ανησυχητικά είναι τα ευρήματα των Zou et al. (2023), οι οποίοι παρουσιάζουν την επίθεση IoTBeholder. Η τεχνική αυτή επιτρέπει σε έναν παθητικό επιτιθέμενο να εξάγει συμπεριφορικά μοτίβα των κατοίκων ενός σπιτιού αποκλειστικά μέσω της ανάλυσης του Wi-Fi traffic. Χωρίς πρόσβαση στο περιεχόμενο των πακέτων, ο επιτιθέμενος μπορεί να εντοπίσει τι είδους συσκευές χρησιμοποιούνται, ποια εφαρμογή ενεργοποιείται και ποια ρουτίνα ακολουθείται. Αυτό υποδηλώνει ότι το profiling μπορεί να λάβει χώρα ακόμη και όταν η επικοινωνία είναι κρυπτογραφημένη, εφόσον παραμένουν διαθέσιμα metadata όπως συχνότητα, μέγεθος και χρονισμός πακέτων.

Στο ίδιο πνεύμα, οι Luo et al. (2020) εξετάζουν πώς η συμφραζόμενη πληροφορία (context-rich data) μπορεί να οδηγήσει σε διαρροή ευαίσθητων λεπτομερειών. Οι συγγραφείς δείχνουν ότι ένας αντίπαλος μπορεί να προσδιορίσει ποιες εφαρμογές χρησιμοποιεί ένας χρήστης σε ένα smart home περιβάλλον, ακόμη και χωρίς πρόσβαση στο περιεχόμενο επικοινωνίας, απλώς συγκρίνοντας μοτίβα κίνησης με γνωστά signatures εφαρμογών. Αυτό αναδεικνύει την ισχύ της ανάλυσης metadata και τον κίνδυνο επιβεβαίωσης δεδομένων χρήσης που δεν προορίζονται για αποκάλυψη.

Παράδειγμα συστημικής διαρροής ιδιωτικότητας αποτελεί και η εργασία των Xu et al. (2019), οι οποίοι εξετάζουν την πλατφόρμα IFTTT ως χαρακτηριστικό ενδιάμεσο σύστημα αυτοματισμών. Η ανάλυση τους δείχνει ότι εφαρμογές και υπηρεσίες που συνδέονται με το smart home μέσω IFTTT έχουν τη δυνατότητα να συλλέξουν πολύ ευρύτερα δεδομένα από αυτά που δηλώνεται στους χρήστες. Οι αυτοματισμοί μπορούν να αποκαλύψουν πλήρη χρονικά μοτίβα χρήσης, όπου η κάθε trigger-action ακολουθία λειτουργεί ως "προφίλ συμπεριφοράς". Οι συγγραφείς καταλήγουν ότι το οικοσύστημα IFTTT οδηγεί σε διαρροές λόγω υπερ-συλλογής και υπερ-εξαγωγής συμφραζομένων.

Η συσσώρευση αυτών των δεδομένων επιτρέπει την κατασκευή μοντέλων συμπεριφοράς υψηλής ακρίβειας. Οι Dilraj et al. (2019) εξετάζουν πώς το behavioral profiling μπορεί να χρησιμοποιηθεί για ανίχνευση ανωμαλιών, αλλά ταυτόχρονα αναγνωρίζουν ότι η καταγραφή λεπτομερών behavioral signatures μπορεί να δημιουργήσει νέους κινδύνους ιδιωτικότητας. Τα μοτίβα συμπεριφοράς που συλλέγονται για άμυνα μπορούν να αποτελέσουν εργαλείο επίθεσης, εφόσον αποκαλύπτουν ακριβείς ρουτίνες και επιτρέπουν τη στοχοποίηση των χρηστών σε κατάλληλες χρονικές στιγμές (π.χ. ώρες απουσίας από το σπίτι).

Η έρευνα των Sanchez et al. (2014) δείχνει ότι οι διαρροές δεν περιορίζονται σε ανάλυση metadata, αλλά μπορούν να προκύψουν και από την απροσεξία ή αδυναμία σχεδιασμού των ασύρματων πρωτοκόλλων που χρησιμοποιούνται στα smart homes. Οι συγγραφείς αναλύουν μια σειρά wireless τεχνολογιών και επιβεβαιώνουν ότι traffic patterns, identification beacons και μη κρυπτογραφημένα headers μπορούν να αποκαλύψουν τύπους συσκευών, συχνότητα χρήσης, ακόμη και προσωπικές συνήθειες. Αυτό αποδεικνύει ότι το profiling δεν είναι απλώς θεωρητικό σενάριο αλλά πρακτική δυνατότητα σε πραγματικά περιβάλλοντα.

Οι τελευταίες εξελίξεις στη βιβλιογραφία εξετάζουν κατά πόσο το profiling μπορεί να χρησιμοποιηθεί και ως στοιχείο ενίσχυσης της ασφάλειας. Η εργασία των Meixiu & Wenhao (2025) προτείνει ένα context-aware intrusion detection model που συνδυάζει behavioral biometrics με device profiling, αξιοποιώντας τα μοτίβα συμπεριφοράς για τον εντοπισμό ανωμαλιών. Παρότι η μελέτη αποδεικνύει ότι η χρήση behavioral signatures ενισχύει την ακρίβεια εντοπισμού επιθέσεων, παραδέχεται ότι παράλληλα αυξάνει τον κίνδυνο αποκάλυψης λεπτομερών δεδομένων σχετικά με την καθημερινότητα των χρηστών, γεγονός που αποτελεί σημαντική πρόκληση για την ιδιωτικότητα.

Αντίστοιχα, ο Garg (2022) προτείνει ένα machine learning πλαίσιο που αξιοποιεί behavioral biometrics για την ενίσχυση της ασφάλειας. Το σύστημα βασίζεται στην παρακολούθηση συγκεκριμένων μοτίβων χρήσης συσκευών, επιβεβαιώνοντας έτσι ότι κάθε χρήστης έχει μοναδικό behavioral αποτύπωμα. Ωστόσο, όπως επισημαίνει ο ίδιος, τέτοιου είδους προσεγγίσεις δημιουργούν «ευαίσθητα βιομετρικά προφίλ», τα οποία

αν διαρρεύσουν μπορούν να χρησιμοποιηθούν για στοχοποιημένη παρακολούθηση ή για την αναγνώριση χρηστών σε πολλαπλά περιβάλλοντα.

Οι Sharma et al. (2025) εξετάζουν ένα παρακλάδι του profiling που αφορά τους prosumers σε έξυπνα ενεργειακά δίκτυα. Η μελέτη τους δείχνει ότι ακόμη και τα δεδομένα των smart meters επαρκούν για τη δημιουργία ακριβών προφίλ χρήσης, όπως το πότε καταναλώνεται ενέργεια, ποια συσκευή ενεργοποιείται, και αν ο χρήστης βρίσκεται στο σπίτι. Η εργασία τονίζει τον κίνδυνο ότι τα δεδομένα αυτά μπορούν να χρησιμοποιηθούν για στοχευμένες επιθέσεις ή για οικονομική εκμετάλλευση μέσω micro-targeting.

Τέλος, οι Kohli et al. (2025) διερευνούν το profiling από την πλευρά της επιστήμης δεδομένων και τονίζουν ότι η συνεχής συλλογή λειτουργικών δεδομένων από smart homes δημιουργεί «ψηφιακούς δίδυμους» των χρηστών. Αυτό σημαίνει ότι ένας επιτιθέμενος, ένας εμπορικός οργανισμός ή ακόμη και ένας πάροχος υπηρεσιών μπορεί να ανακατασκευάσει με ακρίβεια το καθημερινό πρόγραμμα, τις προτιμήσεις και τις συνήθειες των χρηστών. Οι συγγραφείς προειδοποιούν ότι η χρήση τέτοιων προφίλ μπορεί να οδηγήσει σε διακρίσεις, παρακολούθηση, εκβιασμό ή παραβίαση της σωματικής και ψυχολογικής ασφάλειας.

Η βιβλιογραφία αποδεικνύει ότι τα δεδομένα των smart homes, ακόμη και όταν δεν φαίνονται άμεσα προσωπικά, ενέχουν σημαντικούς κινδύνους διαρροής βάσει analysis-through-correlation. Η δημιουργία αναλυτικών behavioral profiles είναι δυνατή μέσω ενεργειακών μοτίβων, Wi-Fi metadata, IFTTT triggers, device activity logs και ασύρματων πρωτοκόλλων. Οι κίνδυνοι περιλαμβάνουν:

- Αναγνώριση ρουτινών και παρουσίας/απουσίας.
- Συμπεράσματα για προσωπικές προτιμήσεις και συμπεριφορές.
- Εντοπισμό μοτίβων που σχετίζονται με υγεία, ύπνο ή ευάλωτες στιγμές.
- Εμπορική εκμετάλλευση μέσω profiling για στοχευμένες διαφημίσεις.
- Εξατομικευμένες κυβερνοεπιθέσεις υψηλής αποτελεσματικότητας.

Η πρόκληση για την επιστημονική κοινότητα είναι να αναπτύξει τεχνικές που διατηρούν τη λειτουργικότητα των smart homes χωρίς να επιτρέπουν τη δημιουργία

τόσο ακριβών προφίλ, ενσωματώνοντας μηχανισμούς απο-ανωνυμοποίησης, obfuscation και data minimization.

3.3.4. Σχέση χρηστικότητας – ασφάλειας: συμβιβασμοί και συμπεριφορικά μοτίβα

Η σχέση μεταξύ χρηστικότητας και ασφάλειας στα συστήματα έξυπνων σπιτιών αποτελεί ένα από τα πιο συζητημένα ζητήματα στη σχεδίαση και υιοθέτηση των τεχνολογιών αυτών. Η καθημερινή εμπειρία των χρηστών διαμορφώνεται τόσο από το πόσο εύχρηστες και αποτελεσματικές είναι οι συσκευές, όσο και από το πώς αντιλαμβάνονται και διαχειρίζονται τους κινδύνους ασφαλείας. Η βιβλιογραφία δείχνει ότι συχνά εμφανίζεται ένα «τρίλημμα» ανάμεσα στη χρηστικότητα, την ασφάλεια και την απόδοση, με συνέπειες που επηρεάζουν τις συμπεριφορές των χρηστών, τις συνήθειες ασφάλειας, αλλά και την τεχνολογική αποδοχή.

Οι Reichherzer et al. (2016) αποτελούν από τους πρώτους που εξετάζουν εμπειρικά τους συμβιβασμούς μεταξύ ασφάλειας, αποδοτικότητας και επεκτασιμότητας σε δίκτυα αισθητήρων έξυπνων σπιτιών. Διαπιστώνουν ότι η εφαρμογή αυστηρών μέτρων ασφαλείας, όπως ισχυρή κρυπτογράφηση και συχνή πιστοποίηση, μειώνει τη λειτουργική απόδοση του δικτύου και αυξάνει την κατανάλωση ενέργειας. Αυτό οδηγεί συχνά σε σχεδιαστικές αποφάσεις όπου οι μηχανικοί επιλέγουν «ελαφρύτερες» λύσεις για χάρη της χρηστικότητας και της ενεργειακής αποδοτικότητας. Η μελέτη επιβεβαιώνει ότι οι τεχνικοί συμβιβασμοί αντικατοπτρίζονται άμεσα στη συμπεριφορά των χρηστών, οι οποίοι αντιμετωπίζουν καθυστερήσεις, δυσκολίες σύνδεσης ή μειωμένη απόκριση όταν ενεργοποιούνται πιο αυστηρές παράμετροι ασφάλειας.

Η αποδοχή τέτοιων συμβιβασμών από τους χρήστες συνδέεται με την αντίληψη για τα κέρδη και τις απώλειες που προκύπτουν από τη χρήση των τεχνολογιών αυτών. Οι Distler et al. (2020) δείχνουν ότι τα χαρακτηριστικά της user experience μπορούν να επηρεάσουν σημαντικά την ανεκτικότητα των χρηστών προς τις υποχωρήσεις στην ιδιωτικότητα και την ασφάλεια. Οι χρήστες που αντιλαμβάνονται υψηλό λειτουργικό όφελος ή άνεση εμφανίζουν μεγαλύτερη διάθεση για αποδοχή privacy trade-offs, ακόμη και όταν δεν κατανοούν πλήρως τους κινδύνους. Ωστόσο, η αποδοχή αυτή δεν είναι απεριόριστη. Όταν η πολυπλοκότητα αυξάνεται ή η καθημερινή εμπειρία επιβαρύνεται, τότε οι χρήστες συχνά μειώνουν τα μέτρα ασφαλείας για να αποκαταστήσουν τη χρηστικότητα.

Το φαινόμενο αυτό συνδέεται άμεσα με την έννοια του *security fatigue*, όπου οι χρήστες κουράζονται από συνεχείς ειδοποιήσεις, απαιτήσεις για ενημερώσεις, αλλαγή κωδικών, ή διαδικασίες επιβεβαίωσης ταυτότητας. Οι Magara & Zhou (2024) επισημαίνουν ότι σε πολλά smart home περιβάλλοντα οι χρήστες νιώθουν επιβαρυμένοι από τις λειτουργίες ασφαλείας, ειδικά όταν αυτές απαιτούν συχνές παρεμβάσεις. Η κούραση αυτή οδηγεί σε φαινόμενα risky behavior, όπως η επαναχρησιμοποίηση κωδικών, η απενεργοποίηση MFA, ή η παραχώρηση πρόσβασης σε συσκευές χωρίς έλεγχο.

Η βιβλιογραφία αναδεικνύει επίσης έναν «κύκλο προσαρμογής» των χρηστών, όπου η αρχική επιφυλακτικότητα προς την ασφάλεια μειώνεται με την πάροδο του χρόνου. Οι Wang et al. (2025) και Regmi et al. (2025) δείχνουν σε ανεξάρτητες αλλά συμπληρωματικές μελέτες ότι οι χρήστες τείνουν να γίνονται σταδιακά πιο ανεκτικοί σε συστήματα συνεχούς αυθεντικοποίησης (continuous authentication), τα οποία αρχικά θεωρούνται παρεμβατικά. Με την εξοικείωση, οι χρήστες προσαρμόζουν τις προσδοκίες τους και θεωρούν τις διαδικασίες ασφάλειας λιγότερο ενοχλητικές, υπό την προϋπόθεση ότι δεν παρεμποδίζουν την καθημερινή λειτουργικότητα του σπιτιού.

Παράλληλα, οι Barbosa et al. (2020) διαπιστώνουν ότι δεν αντιλαμβάνονται όλοι οι χρήστες με τον ίδιο τρόπο τη σημασία της ασφάλειας και της ιδιωτικότητας. Η μελέτη τους εντοπίζει τρεις κύριες κατηγορίες χρηστών: εκείνους που δίνουν προτεραιότητα στη χρηστικότητα, εκείνους που δίνουν προτεραιότητα στην ασφάλεια, και εκείνους που παρουσιάζουν αδιάφορη στάση, είτε λόγω έλλειψης τεχνογνωσίας είτε λόγω μειωμένης αντίληψης κινδύνου. Οι χρήστες με υψηλή τεχνολογική εξοικείωση εμφανίζουν μεγαλύτερη ευαισθησία στα ζητήματα ασφαλείας, αλλά ταυτόχρονα αναζητούν λύσεις που δεν επιβαρύνουν το user experience.

Στο πλαίσιο των smart locks, που αποτελούν χαρακτηριστικό παράδειγμα τεχνολογίας όπου η ασφάλεια και η χρηστικότητα συγκρούονται, ο Hazazi (2024) εξετάζει εις βάθος τις συμπεριφορές και τα εμπειρικά μοτίβα των τελικών χρηστών. Η μελέτη δείχνει ότι όταν οι λειτουργίες ασφαλείας αυξάνουν τη δυσκολία χρήσης (π.χ. καθυστέρηση στο ξεκλείδωμα, ανάγκη για πολλαπλά authentication steps), οι χρήστες τείνουν να απενεργοποιούν τις ασφαλέστερες επιλογές ή να χρησιμοποιούν workaround πρακτικές. Αυτό επιβεβαιώνει τη θεμελιώδη ένταση ανάμεσα σε ευκολία και

προστασία — όσο πιο περίπλοκη η διαδικασία ασφαλείας, τόσο μεγαλύτερη η πιθανότητα οι χρήστες να τη παρακάμπτουν.

Η σύγκρουση αυτή αντικατοπτρίζεται και στη σχεδίαση των IoT δικτύων. Οι Asonze et al. (2024) εξετάζουν πώς η ισχυρή ασφάλεια στα ασύρματα πρωτόκολλα μπορεί να μειώσει την απόδοση AI-driven οικιακών συστημάτων. Οι συγγραφείς δείχνουν ότι υψηλά επίπεδα κρυπτογράφησης, τακτικές ανανεώσεις κλειδιών και αυστηρή επικύρωση πακέτων οδηγούν σε latency, το οποίο γίνεται ιδιαίτερα αισθητό σε εφαρμογές που απαιτούν real-time ανταπόκριση. Με βάση τα ευρήματα, πολλοί πάροχοι τεχνολογίας επιλέγουν «ισορροπημένες ρυθμίσεις» που μειώνουν τη μέγιστη ασφάλεια για να διατηρήσουν αποδεκτή απόδοση.

Ένα άλλο σημαντικό θέμα αφορά την υποκειμενική αντίληψη επιτήρησης από τους χρήστες. Η ανασκόπηση των Percy-Campbell et al. (2024) δείχνει ότι η χρήση έξυπνων καμερών και συσκευών παρακολούθησης μπορεί να δημιουργήσει άγχος ή αίσθηση υπερβολικής έκθεσης, ακόμη και όταν οι χρήστες αναγνωρίζουν τα πλεονεκτήματα ασφάλειας. Σε πολλές περιπτώσεις, οι χρήστες επιλέγουν να απενεργοποιούν λειτουργίες παρακολούθησης όταν βρίσκονται εντός οικίας, γεγονός που αποτυπώνει την ανάγκη για «ευέλικτη ασφάλεια» που σέβεται τα όρια της ιδιωτικής ζωής.

Τέλος, οι Jahid (2025) αναλύουν τον τρόπο με τον οποίο τα AI-powered smart home συστήματα μπορούν να βελτιστοποιήσουν την ισορροπία χρηστικότητας και ασφάλειας. Οι έξυπνοι αλγόριθμοι μπορούν να προσαρμόζουν δυναμικά το επίπεδο ασφάλειας, μειώνοντας τον φόρτο στον χρήστη και ελαχιστοποιώντας το security fatigue. Παρά τις δυνατότητες αυτές, η μελέτη προειδοποιεί ότι η υπερβολική εξάρτηση από την αυτοματοποίηση μπορεί να οδηγήσει σε παθητικότητα των χρηστών και σε μειωμένη επίγνωση κινδύνων — ένα φαινόμενο που ενισχύει τα risky behaviors, καθώς οι χρήστες θεωρούν τις συσκευές «απόλυτα ασφαλείς» χάρη στην τεχνητή νοημοσύνη.

Η βιβλιογραφία δείχνει ότι η σχέση χρηστικότητας – ασφάλειας στα smart homes καθορίζεται από μια σειρά παραμέτρων, μεταξύ των οποίων:

- Η πολυπλοκότητα των διαδικασιών ασφαλείας, που μπορεί να μειώσει την πρόθεση συμμόρφωσης.

- Η αντιληπτή αξία της ασφάλειας, που επηρεάζει την ανοχή των χρηστών σε μειώσεις χρηστικότητας.
- Το security fatigue, που οδηγεί σε χαλαρή συμπεριφορά ή απενεργοποίηση μέτρων.
- Η εξοικείωση με την τεχνολογία, που διαμορφώνει το πώς οι χρήστες ζυγίζουν ευκολία και ασφάλεια.
- Η υποκειμενική αίσθηση ιδιωτικότητας και επιτήρησης, η οποία συχνά υπερισχύει των αντικειμενικών κινδύνων.
- Η απόδοση του συστήματος, η οποία μπορεί να υποβαθμιστεί από ενισχυμένα μέτρα προστασίας.

Η κατανόηση αυτών των παραγόντων είναι κρίσιμη για τη σχεδίαση έξυπνων σπιτιών που επιτυγχάνουν μια βιώσιμη ισορροπία ανάμεσα στην ασφάλεια και τη χρηστικότητα, αποτρέποντας ταυτόχρονα τις συμπεριφορές που θέτουν σε κίνδυνο τους χρήστες.

3.3.5. Εμπειρικές έρευνες για τις ανησυχίες και τις προσδοκίες των χρηστών

Οι εμπειρικές έρευνες γύρω από τις ανησυχίες και τις προσδοκίες των χρηστών στα έξυπνα σπίτια έχουν αναδείξει μια σύνθετη πραγματικότητα, όπου η επιθυμία για άνεση, αυτοματοποίηση και ενεργειακή αποδοτικότητα συγκρούεται με τον φόβο της παρακολούθησης, της απώλειας ιδιωτικότητας και της ανεπαρκούς διαχείρισης δεδομένων. Οι μελέτες – ποιοτικές και ποσοτικές – προσφέρουν μια πολυεπίπεδη εικόνα σχετικά με το πώς οι χρήστες κατανοούν τους κινδύνους, πώς ερμηνεύουν τις δυνατότητες των συστημάτων έξυπνου σπιτιού και ποιες προσδοκίες διαμορφώνουν ως προς τη χρήση και την προστασία των προσωπικών τους πληροφοριών.

Στο έργο των Schomakers et al. (2021), η εμπιστοσύνη και η ιδιωτικότητα αποτελούν τους δύο βασικούς πυλώνες γύρω από τους οποίους περιστρέφονται οι προτιμήσεις των χρηστών για την αυτοματοποίηση του σπιτιού. Η μελέτη δείχνει ότι οι χρήστες αναμένουν από τις συσκευές να λειτουργούν με προβλέψιμο και κατανοητό τρόπο, ενώ επιθυμούν σαφή πληροφόρηση σχετικά με το είδος των δεδομένων που συλλέγονται και τους σκοπούς χρήσης τους. Παράλληλα, οι συμμετέχοντες εκφράζουν επιφυλάξεις

για συσκευές που διατηρούν συνεχή πρόσβαση στις δραστηριότητές τους, επισημαίνοντας ότι ο φόβος παρακολούθησης ή μη εξουσιοδοτημένης χρήσης δεδομένων μειώνει την προθυμία τους να τις υιοθετήσουν.

Σε αντίστοιχο πλαίσιο, η έρευνα των Guhr et al. (2020) καταγράφει ότι οι ανησυχίες για την ιδιωτικότητα δεν είναι μόνο διάχυτες αλλά και διαφοροποιημένες: αφορούν τόσο τους τεχνικούς κινδύνους (π.χ. hacking, διαρροή δεδομένων) όσο και κοινωνικές διαστάσεις, όπως η πιθανότητα ανεπιθύμητης επιτήρησης από τρίτους. Οι συγγραφείς αναδεικνύουν ένα σημαντικό εύρημα: οι χρήστες συχνά δεν έχουν πλήρη κατανόηση του τρόπου λειτουργίας των έξυπνων συσκευών, γεγονός που αυξάνει την αντιληπτή αβεβαιότητα και, κατά συνέπεια, τις ανησυχίες τους. Η έλλειψη διαφάνειας και η περίπλοκη ή δυσνόητη παρουσίαση των πολιτικών ιδιωτικότητας ενισχύουν την πεποίθηση ότι οι συσκευές ενδέχεται να καταχραστούν τα προσωπικά δεδομένα.

Στροφή προς τις ανησυχίες από πλευράς επιστημονικής κοινότητας εμφανίζεται στην έρευνα των Birchley et al. (2017), η οποία εξετάζει τις ηθικές ανησυχίες των ίδιων των ερευνητών που αναπτύσσουν smart home τεχνολογίες, ιδιαίτερα στον τομέα της υγείας. Η μελέτη αποκαλύπτει ότι ακόμη και οι τεχνολόγοι ανησυχούν για την ενδεχόμενη υπέρβαση ορίων στην ιδιωτική ζωή, ιδιαίτερα όταν τα συστήματα αποσκοπούν σε συνεχή παρακολούθηση ηλικιωμένων ή ασθενών. Οι ερευνητές επισημαίνουν ότι οι χρήστες μπορεί να αισθάνονται ευάλωτοι ή εκτεθειμένοι, καθώς οι τεχνολογίες αυτές συλλέγουν μεγάλης λεπτομέρειας δεδομένα που μπορούν να αποκαλύψουν ευαίσθητες πτυχές της καθημερινότητας. Έτσι, η μελέτη υπογραμμίζει ότι οι ηθικές ανησυχίες δεν εντοπίζονται μόνο στις αντιλήψεις των χρηστών, αλλά και στην ίδια την κοινότητα που δημιουργεί τις τεχνολογίες.

Παράλληλα, η εργασία των Chalhoub et al. (2021) εξετάζει την εμπειρία των χρηστών μέσα από μια μακροχρόνια μελέτη που αποκαλύπτει ότι οι ανησυχίες για την ιδιωτικότητα συχνά ενισχύονται με την πάροδο του χρόνου. Αν και αρχικά οι χρήστες μπορεί να υποτιμούν τους κινδύνους ή να μην τους κατανοούν πλήρως, σταδιακά γίνονται πιο ευαισθητοποιημένοι καθώς τα συστήματα λειτουργούν και αλληλεπιδρούν με την καθημερινή ζωή. Οι ερευνητές εντοπίζουν συχνά φαινόμενα «αναγκασμένης συναίνεσης», όπου τα συστήματα δεν παρέχουν δυνατότητα άρνησης ή επιλογής σε βασικές λειτουργίες παρακολούθησης. Αυτό οδηγεί πολλούς χρήστες να νιώθουν ότι

έχουν περιορισμένο έλεγχο, γεγονός που υπονομεύει την εμπιστοσύνη τους στα έξυπνα οικοσυστήματα.

Η πρόβλεψη των προτιμήσεων των χρηστών αποτελεί επίσης αντικείμενο μελέτης. Οι Barbosa et al. (2019) διερευνούν το πώς μεταβάλλονται οι προτιμήσεις των χρηστών ως προς τις ρυθμίσεις ιδιωτικότητας μέσα από εναλλακτικά σενάρια. Η μελέτη δείχνει ότι η στάση των χρηστών δεν είναι στατική· αντιθέτως, μεταβάλλεται ανάλογα με το πλαίσιο, τον σκοπό χρήσης της συσκευής και τον αντιληπτό κίνδυνο. Οι συγγραφείς αναφέρουν ότι οι χρήστες εμφανίζουν υψηλότερα επίπεδα ανησυχίας όταν τα δεδομένα μπορούν να αποκαλύψουν προσωπικές συνήθειες ή συμπεριφορές, ενώ είναι περισσότερο διατεθειμένοι να μοιραστούν δεδομένα που θεωρούν μη ευαίσθητα ή γενικής χρήσης. Η μεταβλητότητα αυτή καθιστά δύσκολη τη θέσπιση ενιαίων μηχανισμών προστασίας ιδιωτικότητας που να ανταποκρίνονται στις ανάγκες όλων.

Η ανάγκη για περισσότερο έλεγχο των δεδομένων αποτελεί κεντρικό συμπέρασμα της μελέτης των Chhetri & Motti (2022), οι οποίοι εξετάζουν τη σχεδίαση user-centric privacy controls. Οι συγγραφείς υποστηρίζουν ότι η έλλειψη διαφανών και κατανοητών εργαλείων διαχείρισης δεδομένων αποτελεί βασική πηγή ανησυχίας των χρηστών. Η έρευνα καταδεικνύει ότι οι χρήστες επιθυμούν μηχανισμούς που να τους επιτρέπουν να επιλέγουν ρητά τι συλλέγεται, πότε και από ποιες συσκευές. Όπως υποστηρίζουν, η ύπαρξη τέτοιων εργαλείων δεν ενισχύει μόνο την εμπιστοσύνη αλλά και την προθυμία για υιοθέτηση.

Πέρα από τις ανησυχίες, οι μελέτες εξετάζουν και τις προσδοκίες των χρηστών. Η ποσοτική ανάλυση των Gu et al. (2019) για την πρόθεση συνέχισης χρήσης smart home υπηρεσιών δείχνει ότι οι χρήστες αναμένουν συστήματα που είναι αξιόπιστα, συνεπή στη λειτουργία τους, εύκολα στη χρήση και προσαρμόσιμα στις ανάγκες τους. Ωστόσο, οι συγγραφείς επισημαίνουν ότι οι ανησυχίες για ιδιωτικότητα μπορούν να περιορίσουν την προθυμία συνέχισης χρήσης, ακόμη και όταν το σύστημα είναι τεχνικά άρτια. Το εύρημα αυτό επιβεβαιώνει ότι η εμπιστοσύνη αποτελεί κρίσιμο παράγοντα για τη μακροπρόθεσμη αποδοχή των τεχνολογιών.

Μια πιο «κοινωνικά παρατηρησιακή» προσέγγιση υιοθετείται στην πρόσφατη εργασία των Protick et al. (2024), η οποία αναλύει τις αντιδράσεις και ανησυχίες χρηστών μέσα από διαδικτυακές αξιολογήσεις προϊόντων smart home. Η μελέτη δείχνει ότι οι

ανησυχίες για την ασφάλεια και την ιδιωτικότητα είναι όχι μόνο συχνές αλλά και ιδιαίτερα έντονες σε περιπτώσεις συσκευών με κάμερες, μικρόφωνα ή λειτουργίες απομακρυσμένης πρόσβασης. Πολλοί χρήστες εκφράζουν φόβο ότι τα δεδομένα τους αποθηκεύονται χωρίς τη συγκατάθεσή τους, ότι υπάρχει ενδεχόμενο παραβίασης από τρίτους ή ακόμη και ότι οι ίδιες οι εταιρείες εκμεταλλεύονται τις πληροφορίες για εμπορικούς σκοπούς. Αυτή η «αυθόρμητη» πηγή δεδομένων υπογραμμίζει ότι οι ανησυχίες δεν περιορίζονται στο ακαδημαϊκό περιβάλλον, αλλά αποτελούν πραγματικές εμπειρίες και προτεραιότητες των καθημερινών χρηστών.

Οι εμπειρικές μελέτες συγκλίνουν σε ορισμένα κοινά συμπεράσματα:

- Η ιδιωτικότητα παραμένει ο πιο κρίσιμος παράγοντας ανησυχίας. Οι χρήστες φοβούνται την κατάχρηση δεδομένων, την παρακολούθηση και την έλλειψη ελέγχου.
- Η εμπιστοσύνη προς τις εταιρείες και τους παρόχους είναι εύθραυστη. Η έλλειψη διαφάνειας ή ξεκάθαρων επιλογών συναίνεσης μειώνει την αποδοχή.
- Οι προσδοκίες των χρηστών είναι υψηλές και πολυδιάστατες. Θέλουν έξυπνες λειτουργίες, αλλά χωρίς να θυσιάσουν την ασφάλεια ή την ιδιωτικότητα.
- Η εμπειρία χρήσης μπορεί να μεταβάλει τις αντιλήψεις τους. Με τον χρόνο, οι χρήστες είτε αναπτύσσουν μεγαλύτερη εμπιστοσύνη είτε γίνονται πιο καχύποπτοι, ανάλογα με την ποιότητα της τεχνολογίας.
- Ο έλεγχος των δεδομένων αποτελεί κεντρική απαίτηση. Οι χρήστες ζητούν granular privacy controls και περισσότερη αυτονομία στη διαχείριση των πληροφοριών τους.

Η κατανόηση των ανησυχιών και προσδοκιών των χρηστών αποτελεί προϋπόθεση για τη σχεδίαση έξυπνων σπιτιών που συνδυάζουν χρηστικότητα, εμπιστοσύνη και σεβασμό στην ιδιωτικότητα. Οι εμπειρικές αυτές έρευνες αποδεικνύουν ότι η τεχνολογία δεν μπορεί να είναι κοινωνικά ουδέτερη: οι χρήστες επιθυμούν να αισθάνονται ότι έχουν τον έλεγχο και ότι προστατεύονται σε ένα οικοσύστημα που βρίσκεται ολοένα και πιο βαθιά ενσωματωμένο στον προσωπικό τους χώρο.

3.4. Συγκριτική ανάλυση ευρημάτων και κύριων τάσεων

Η συγκριτική αξιολόγηση των προτεινόμενων λύσεων ασφάλειας για έξυπνα σπίτια αποκαλύπτει μια σύνθετη και συχνά αντιφατική εικόνα, όπου οι τεχνικές δυνατότητες, οι επιχειρησιακοί περιορισμοί και οι ανθρώπινες συμπεριφορές αλληλεπιδρούν με τρόπο που καθορίζει την πραγματική αποτελεσματικότητα των μηχανισμών προστασίας. Τα ευρήματα από τα προηγούμενα κεφάλαια αναδεικνύουν ότι οι λύσεις που προτείνει η βιβλιογραφία στο πεδίο της ασφάλειας IoT (κεφάλαιο 3.2) είναι εκτενείς και τεχνικά ώριμες. Ωστόσο, όταν εξεταστούν υπό το πρίσμα των πραγματικών επιθέσεων στα επικοινωνιακά πρωτόκολλα (κεφάλαιο 3.1) και των συμπεριφορικών μοτίβων των χρηστών (κεφάλαιο 3.3), καθίσταται σαφές ότι η αποτελεσματικότητά τους περιορίζεται από παράγοντες που ξεπερνούν την καθαρά τεχνολογική διάσταση.

Ένα πρώτο σημείο σύγκρισης αφορά τη σχέση μεταξύ ευπαθειών των συσκευών και των μηχανισμών αυθεντικοποίησης. Οι αδυναμίες που καταγράφονται σε κάμερες, αισθητήρες και smart locks συχνά συνδέονται με ανεπαρκείς πολιτικές κωδικών, απουσία πολυπαραγοντικής αυθεντικοποίησης και ελλιπείς μηχανισμούς ελέγχου πρόσβασης. Ενώ η βιβλιογραφία προτείνει ισχυρούς μηχανισμούς, όπως MFA, βιομετρικά δεδομένα και αυστηρότερες πολιτικές κωδικών, στην πράξη η υιοθέτηση από τους χρήστες παραμένει χαμηλή. Αυτό οφείλεται είτε στη δυσκολία χρήσης αυτών των μεθόδων είτε στην περιορισμένη κατανόηση των κινδύνων. Οι μελέτες της Distler et al. (2020) και άλλων ερευνητών του κεφαλαίου 3.3 δείχνουν ότι όταν οι διαδικασίες αυθεντικοποίησης γίνονται περίπλοκες, οι χρήστες τείνουν να τις παρακάμπτουν, υποβαθμίζοντας έτσι την ασφάλεια που προσφέρουν οι τεχνικές λύσεις. Επομένως, παρότι οι μηχανισμοί πρόσβασης αποτελούν κρίσιμη άμυνα απέναντι στις ευπάθειες που εντοπίστηκαν στο κεφάλαιο 3.1, η πραγματική τους αποτελεσματικότητα περιορίζεται από θέματα χρηστικότητας και συμπεριφορικής συμμόρφωσης.

Αντίστοιχα, τα κρυπτογραφικά πρωτόκολλα που προτείνονται στο κεφάλαιο 3.2.2 αποτελούν μια σημαντική ασπίδα απέναντι στις επιθέσεις σε επικοινωνιακά πρωτόκολλα IoT, όπως Wi-Fi, Zigbee, Z-Wave και Bluetooth. Οι επιθέσεις τύπου MITM, spoofing και replay που περιγράφονται στο κεφάλαιο 3.1.2 μπορούν πράγματι να μετριαστούν μέσω ισχυρής κρυπτογράφησης, ασφαλούς διαχείρισης κλειδιών και

lightweight αλγορίθμων που προσαρμόζονται στους περιορισμούς των IoT συσκευών. Η σύγκριση, όμως, αποκαλύπτει ότι οι τεχνολογικές αυτές λύσεις προσκρούουν σε εγγενή περιορισμένα χαρακτηριστικά των συσκευών, όπως περιορισμένη υπολογιστική ισχύς, μικρή διάρκεια ζωής μπαταρίας και ασύμβατες υλοποιήσεις σε διαφορετικά πρωτόκολλα. Επιπλέον, οι μελέτες χρήσης δείχνουν ότι η κρυπτογράφηση, παρότι τεχνικά αποτελεσματική, παραμένει μια «αόρατη» λειτουργία για τον τελικό χρήστη, ο οποίος σπάνια κατανοεί το περιεχόμενο και τη σημασία της. Έτσι, η αποτελεσματικότητα των κρυπτογραφικών πρωτοκόλλων μειώνεται όταν οι χρήστες δεν ενεργοποιούν προαιρετικές λειτουργίες ασφάλειας ή δεν εφαρμόζουν ενημερώσεις που είναι κρίσιμες για την επίλυση γνωστών ευπαθειών.

Τα συστήματα IDS/IPS που περιγράφονται στην ενότητα 3.2.3 αποτελούν από τις πιο εξελιγμένες τεχνικές άμυνας απέναντι σε εισβολές και ανωμαλίες δικτύου. Η σύγκριση με τις επιθέσεις που παρουσιάστηκαν στα κεφάλαια 3.1.3 και 3.1.4 δείχνει ότι τα IDS/IPS μπορούν να ανιχνεύσουν με μεγάλη ακρίβεια ύποπτες συμπεριφορές, όπως spoofing, MITM και DoS. Ωστόσο, παρά την υψηλή τεχνική αποτελεσματικότητα, στην πραγματικότητα συναντούν σημαντικά εμπόδια. Πολλά μοντέλα απαιτούν ισχυρή επεξεργαστική ισχύ που απουσιάζει από τις περισσότερες συσκευές smart home. Επιπλέον, τα συστήματα που βασίζονται σε ML παρουσιάζουν συχνά μεγάλο αριθμό false positives, γεγονός που κουράζει τους χρήστες και μειώνει την εμπιστοσύνη τους στη λειτουργία του συστήματος. Η σύγκριση με τα συμπεριφορικά ευρήματα του κεφαλαίου 3.3 δείχνει ότι οι χρήστες έχουν περιορισμένη ανοχή σε συστήματα που παρεμβαίνουν συχνά ή αυξάνουν τον γνωστικό φόρτο, κάτι που οδηγεί στην απενεργοποίηση σημαντικών λειτουργιών ασφαλείας.

Οι μέθοδοι τεχνητής νοημοσύνης και machine learning, όπως αυτές περιγράφονται στην ενότητα 3.2.4, αποτελούν ίσως τη μεγαλύτερη τεχνολογική πρόοδο στον τομέα της ασφάλειας των έξυπνων σπιτιών. Τα προηγμένα συστήματα πρόβλεψης, ταξινόμησης και ανίχνευσης ανωμαλιών μπορούν να εντοπίσουν επιθέσεις πολύ πριν γίνουν αντιληπτές από τον χρήστη ή ακόμη και από παραδοσιακά συστήματα άμυνας. Όμως η σύγκριση με τα ευρήματα του κεφαλαίου 3.3 αναδεικνύει μια σημαντική διάσταση: οι ML τεχνικές απαιτούν τη συλλογή και ανάλυση μεγάλου όγκου δεδομένων, γεγονός που αυξάνει τις ανησυχίες των χρηστών σχετικά με το profiling

και τις παραβιάσεις ιδιωτικότητας. Ενώ οι τεχνικές αυτές είναι ιδιαίτερα αποτελεσματικές για την αντιμετώπιση επιθέσεων όπως αυτές του κεφαλαίου 3.1.3, οι χρήστες συχνά δυσπιστούν απέναντι στη συνεχή παρακολούθηση που προϋποθέτουν. Οι ανησυχίες αυτές παρουσιάζονται έντονα στις μελέτες του κεφαλαίου 3.3.5, όπου πολλοί χρήστες εκφράζουν φόβο για την κατάχρηση των προσωπικών τους δεδομένων από κατασκευαστές ή τρίτους.

Η πιο ολιστική και θεωρητικά συνεκτική λύση στη βιβλιογραφία προέρχεται από τις αρχιτεκτονικές ασφαλούς σχεδιασμού, secure-by-design και privacy-by-design, που συζητήθηκαν στο κεφάλαιο 3.2.5. Η σύγκριση με τα ευρήματα των άλλων ενοτήτων δείχνει ότι οι αρχιτεκτονικές αυτές αντιμετωπίζουν τις αδυναμίες σε συσκευές και πρωτόκολλα (3.1), ενώ ταυτόχρονα απαντούν στις ανησυχίες και προσδοκίες των χρηστών (3.3). Η ενσωμάτωση της ασφάλειας από το στάδιο του σχεδιασμού προσφέρει μια πιο δομική προσέγγιση, μειώνοντας την ανάγκη για περίπλοκες επανορθωτικές λύσεις και περιορίζοντας τη συλλογή περιττών δεδομένων. Παρά τα πλεονεκτήματα, όμως, αυτές οι αρχιτεκτονικές παραμένουν δύσκολες στην υλοποίηση λόγω κόστους, έλλειψης τυποποίησης και απροθυμίας κατασκευαστών να αναθεωρήσουν υφιστάμενα μοντέλα παραγωγής.

Η συγκριτική αποτίμηση δείχνει ότι η τεχνική αποτελεσματικότητα μιας λύσης δεν εξασφαλίζει την υιοθέτησή της ούτε την πραγματική προστασία των χρηστών. Οι πιο τεχνολογικά προηγμένες λύσεις – όπως ML-based IDS/IPS και advanced cryptography – είναι αποτελεσματικές σε εργαστηριακές συνθήκες αλλά συχνά δύσχρηστες, αδιαφανείς ή απαιτητικές για τους χρήστες. Αντίθετα, οι αρχιτεκτονικές secure-by-design είναι οι πιο πολλά υποσχόμενες σε επίπεδο μακροπρόθεσμης προστασίας, αλλά δεν έχουν ακόμη ευρεία βιομηχανική εφαρμογή. Η γενική τάση δείχνει ότι η πραγματική ασφάλεια των smart homes θα επιτευχθεί μόνο με συνδυασμό τεχνικών εργαλείων, δομικής αναθεώρησης του τρόπου σχεδίασης των συσκευών και προσέγγιση που λαμβάνει σοβαρά υπόψη τις ανάγκες, τα όρια και τις συμπεριφορές των τελικών χρηστών.

4. Συμπεράσματα

Το πεδίο των έξυπνων σπιτιών εξελίσσεται με ιδιαίτερα γρήγορους ρυθμούς, μετασχηματίζοντας τον τρόπο με τον οποίο οι χρήστες αλληλεπιδρούν με τις καθημερινές τους δραστηριότητες. Η συσσώρευση ερευνητικού έργου σχετικά με την ασφάλεια και την ιδιωτικότητα σε αυτά τα περιβάλλοντα αποκαλύπτει ένα σύστημα υψηλής πολυπλοκότητας, στο οποίο η τεχνολογία, η ανθρώπινη συμπεριφορά και οι αρχές κυβερνοασφάλειας συνυπάρχουν μερικές φορές αρμονικά και άλλες συγκρουσιακά. Η ανασκόπηση των διαθέσιμων μελετών καταδεικνύει ότι το έξυπνο σπίτι δεν αποτελεί απλώς ένα σύνολο συνδεδεμένων συσκευών, αλλά ένα κοινωνικοτεχνικό οικοσύστημα, στο οποίο η ασφάλεια εξαρτάται τόσο από τις τεχνικές υποδομές όσο και από τις ανθρώπινες στάσεις, τη γνώση, τις προσδοκίες και τα όρια ανοχής στους κινδύνους.

Παρά τις τεχνολογικές εξελίξεις σε επίπεδο πρωτοκόλλων επικοινωνίας, αλγορίθμων ανίχνευσης εισβολών και προσεγγίσεων ασφαλούς σχεδιασμού, εξακολουθούν να υπάρχουν σημαντικές προκλήσεις που δυσχεραίνουν την πλήρη κατοχύρωση της ιδιωτικότητας και της ασφάλειας. Τα ερευνητικά δεδομένα αποδεικνύουν ότι οι έξυπνες συσκευές – από αισθητήρες έως κάμερες και έξυπνες κλειδαριές – παρουσιάζουν ευπάθειες που συχνά γίνονται αντιληπτές μόνο μετά από εξειδικευμένες δοκιμές ή πραγματικά περιστατικά επίθεσης. Την ίδια στιγμή, οι χρήστες υιοθετούν καθοριστικό ρόλο, καθώς η συμπεριφορά τους μπορεί να ενισχύσει ή να αποδυναμώσει την ασφάλεια του συστήματος.

Με βάση αυτά τα δεδομένα, το παρόν κεφάλαιο επιχειρεί μια ενιαία σύνθεση των βασικών συμπερασμάτων, εντοπίζει τις κοινές θεματικές γραμμές της βιβλιογραφίας και αναδεικνύει τους περιορισμούς που εξακολουθούν να υπάρχουν, τόσο τεχνικούς όσο και μεθοδολογικούς.

Ένα από τα πιο εμφανή συμπεράσματα αφορά την εγγενή πολυπλοκότητα του οικοσυστήματος των smart homes. Η ασφάλεια δεν αποτελεί απλώς ένα τεχνικό ζήτημα που λύνεται με ένα κατάλληλο πρωτόκολλο ή έναν αλγόριθμο. Αντίθετα, προκύπτει από μια σειρά διαστρωματωμένων παραγόντων: αδυναμίες λογισμικού και υλικού, τρωτά σημεία στα πρωτόκολλα ασύρματης επικοινωνίας, ανθρώπινες συμπεριφορές,

προβληματική διαχείριση δεδομένων, και ελλείψεις στη νομοθεσία και στη διακυβέρνηση προσωπικών πληροφοριών.

Το δεύτερο κρίσιμο συμπέρασμα είναι ότι οι χρήστες συχνά βρίσκονται σε μια κατάσταση γνωσιακής ασυμμετρίας απέναντι στις τεχνολογίες smart home. Δεν κατανοούν πλήρως το πώς λειτουργούν οι συσκευές, τι δεδομένα συλλέγουν, πώς αυτά αποθηκεύονται ή διαμοιράζονται, και ποιες είναι οι πιθανές συνέπειες σε περίπτωση παραβίασης. Αυτή η άγνοια οδηγεί είτε σε υπερβολική ανησυχία είτε – συχνότερα – σε υποτίμηση των κινδύνων και σε συμπεριφορές που υπονομεύουν την ασφάλεια, όπως η χρήση αδύναμων κωδικών, η απενεργοποίηση κρίσιμων λειτουργιών ασφαλείας ή η παροχή πρόσβασης σε τρίτους χωρίς έλεγχο.

Παράλληλα, η βιβλιογραφία αναδεικνύει ότι η ασφάλεια και η ιδιωτικότητα συχνά θυσιάζονται χάριν της χρηστικότητας. Οι χρήστες προτιμούν συστήματα απλά στη χρήση, γρήγορα στη λειτουργία και απρόσκοπτα στην καθημερινότητα. Κάθε πρόσθετο επίπεδο ασφαλείας που επιβαρύνει τη λειτουργικότητα – όπως το MFA, οι περίπλοκες ρυθμίσεις ή οι συνεχείς ειδοποιήσεις – οδηγεί συχνά σε μείωση της συμμόρφωσης, γεγονός που επιτρέπει την ανάπτυξη φαινομένων security fatigue και risky behavior.

Ένα ακόμη σημαντικό συμπέρασμα αφορά την εντεινόμενη δυνατότητα ανάδειξης προφίλ χρηστών μέσω ανάλυσης των δεδομένων που παράγονται από τις συσκευές. Μελέτες έχουν δείξει ότι τα δεδομένα κίνησης, φωτισμού, κατανάλωσης ενέργειας ή χρήσης εφαρμογών μπορούν να αποκαλύψουν με μεγάλη ακρίβεια πρότυπα συμπεριφοράς, συνήθειες ή ακόμη και απουσίες από το σπίτι. Αυτή η πραγματικότητα δημιουργεί κινδύνους όχι μόνο τεχνικής αλλά και κοινωνικής φύσης, καθώς ανοίγει τον δρόμο για αθέμιτο profiling ή ακόμη και στοχευμένες επιθέσεις.

Τέλος, η έρευνα επιβεβαιώνει ότι η προληπτική ενσωμάτωση αρχών secure-by-design και privacy-by-design αποτελεί τη μόνη μακροπρόθεσμα βιώσιμη λύση. Η ασφάλεια δεν μπορεί να αποτελεί πρόσθετο επίπεδο που εφαρμόζεται εκ των υστέρων, αλλά πρέπει να ενσωματώνεται στον πυρήνα της αρχιτεκτονικής των συσκευών και των πλατφορμών.

Η βιβλιογραφία παρουσιάζει αξιοσημείωτη σύγκλιση σε ορισμένα θεματικά μοτίβα, παρά το εύρος των τεχνολογιών και των μεθοδολογιών που εξετάζονται. Η

ιδιωτικότητα είναι ο πιο κρίσιμα επηρεαζόμενος τομέας. Ανεξάρτητα από το είδος της συσκευής ή της επίθεσης, η παραβίαση της ιδιωτικότητας καταγράφεται ως ο κίνδυνος με τον μεγαλύτερο αντίκτυπο στον χρήστη. Οι μελέτες δείχνουν ότι το smart home δημιουργεί ένα περιβάλλον όπου η συλλογή δεδομένων είναι συνεχής, αδιάλειπτη και συχνά δυσδιάκριτη. Αυτό οδηγεί σε συστηματική ανασφάλεια των χρηστών ως προς το ποιος έχει πρόσβαση στα δεδομένα τους και για πόσο χρόνο.

Η τεχνολογία ασύρματης επικοινωνίας αποτελεί βασικό σημείο ευπάθειας. Οι επιθέσεις στα πρωτόκολλα Wi-Fi, Zigbee, Z-Wave και Bluetooth είναι επαναλαμβανόμενο θέμα σε πλήθος ερευνών. Η κοινή γραμμή των μελετών είναι ότι τα πρωτόκολλα αυτά σχεδιάστηκαν συχνά με προτεραιότητα στην ενεργειακή αποδοτικότητα και όχι στην ασφάλεια, γεγονός που οδηγεί σε μια σειρά από δομικά τρωτά σημεία. Οι χρήστες εμφανίζουν σημαντικές διαφοροποιήσεις ανάλογα με την τεχνογνωσία, την ηλικία, την κοινωνική ομάδα και την εμπειρία με την τεχνολογία. Αν και οι ανησυχίες για παρακολούθηση και απώλεια ελέγχου εμφανίζονται σε όλες τις ομάδες, οι πιο εξοικειωμένοι χρήστες προβάλλουν πιο σύνθετες απαιτήσεις ασφάλειας, ενώ οι λιγότερο τεχνολογικά καταρτισμένοι τείνουν να υποτιμούν τους κινδύνους.

Η αυτοματοποίηση μέσω AI και η χρήση machine learning ενισχύουν τις δυνατότητες ασφάλειας, αλλά ταυτόχρονα αυξάνουν την αδιαφάνεια. Παρότι οι αλγόριθμοι αυτοί προσφέρουν υψηλή ακρίβεια στην ανίχνευση ανωμαλιών, η πολυπλοκότητά τους καθιστά δύσκολη την κατανόηση του τρόπου λήψης αποφάσεων και δημιουργεί νέα ερωτήματα για την ιδιωτικότητα. Τα πραγματικά περιστατικά επιθέσεων επιβεβαιώνουν ότι οι θεωρητικές αδυναμίες μεταφράζονται σε πρακτικές απειλές. Από πειραματικές επιθέσεις σε smart locks μέχρι ανίχνευση συνηθειών μέσω Wi-Fi traffic, οι μελέτες δείχνουν ότι οι κίνδυνοι δεν είναι μόνο θεωρητικοί, αλλά άμεσα εφαρμόσιμοι σε πραγματικά σπίτια.

Παρά τον πλούτο της, η υπάρχουσα βιβλιογραφία παρουσιάζει ορισμένους περιορισμούς που καθιστούν αναγκαία τη διεύρυνση της έρευνας. Οι περισσότερες έρευνες είναι διατομεακές και δεν εξετάζουν πώς οι στάσεις και ανησυχίες των χρηστών μεταβάλλονται σε βάθος χρόνου. Σε ένα περιβάλλον τόσο δυναμικό, όπου οι τεχνολογίες και οι απειλές αλλάζουν γρήγορα, η απουσία

longitudinal studies αποτελεί σημαντικό κενό. Πολλές μελέτες βασίζονται σε εργαστηριακές προσομοιώσεις ή περιορισμένα dataset. Αυτό μειώνει την εξωτερική εγκυρότητα των συμπερασμάτων, καθώς τα πραγματικά smart homes εμφανίζουν πιο πολύπλοκη αλληλεπίδραση μεταξύ συσκευών, χρηστών και δικτύων. Οι περισσότερες έρευνες εστιάζουν σε τεχνολογικά εξοικειωμένους χρήστες ή σε περιορισμένες γεωγραφικές περιοχές. Λείπουν μελέτες που να εξετάζουν κοινωνικές μειονότητες, ηλικιωμένους, παιδιά ή άτομα με περιορισμένη πρόσβαση σε τεχνολογικά μέσα. Πολλές εργασίες χρησιμοποιούν τους δύο όρους εναλλακτικά, δημιουργώντας συγχύσεις ως προς τα ακριβή όρια και τις απαιτήσεις του καθενός. Χρειάζεται σαφέστερη θεωρητική πλαισίωση. Παρότι πολλές μελέτες αναγνωρίζουν τη σημασία της ανθρώπινης συμπεριφοράς, λίγες εξερευνούν εις βάθος τον τρόπο με τον οποίο συγκεκριμένες σχεδιαστικές αποφάσεις διαμορφώνουν ή επηρεάζουν τις συμπεριφορές αυτές.

Η ερευνητική εικόνα που προκύπτει είναι ξεκάθαρη: η ασφάλεια και η ιδιωτικότητα στα έξυπνα σπίτια απαιτούν μια ολιστική προσέγγιση. Η τεχνολογία από μόνη της δεν αρκεί, όπως δεν αρκεί και η αλλαγή συμπεριφοράς των χρηστών. Το μέλλον της ασφάλειας στα smart homes θα εξαρτηθεί από την ικανότητα των σχεδιαστών να ενσωματώνουν ασφαλείς αρχιτεκτονικές από την αρχή, από την ανάπτυξη διαφανούς και κατανοητής διαχείρισης δεδομένων, και από την ουσιαστική συμμετοχή των χρηστών στη διαδικασία λήψης αποφάσεων για την ιδιωτικότητα τους.

Βιβλιογραφία

1NCE. (2024). *IoT cybersecurity landscape in 2024*. Διαθέσιμο στο: https://www.1nce.com/en-eu/resources/news/blog/iot-cybersecurity-landscape Ανάκτηση στις 26/11/2025.

Ab Rahman, A. B., & Azamuddin, R. (2015). Comparison of internet of things (IoT) data link protocols. *Technical report, Technical report, Washington University in St Louis*, 1-21.

Abduhari, E. S., Shaik, T. C., Adidul, A. B., Ladja, J. H., Saliddin, E. S., Adin, A. J., ... & Tahil, S. K. (2025). Access Control Mechanisms and Their Role in Preventing Unauthorized Data Access: A Comparative Analysis of RBAC, MFA, and Strong Passwords. *Natural Sciences Engineering and Technology Journal*, *5*(1), 418-430.

Abdullah, T. A., Ali, W., Malebary, S., & Ahmed, A. A. (2019). A review of cyber security challenges attacks and solutions for Internet of Things based smart home. *Int. J. Comput. Sci. Netw. Secur*, *19*(9), 139.

Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2020, November). An efficient lightweight cryptographic algorithm for IoT security. In *International Conference on Information and Communication Technology and Applications* (pp. 444-456). Cham: Springer International Publishing.

Abid, M. K., Qadir, M., Farid, S., & Alam, M. (2022). Iot environment security and privacy for smart homes. *Journal of Information Communication Technologies and Robotic Applications*, *13*(1), 15-22.

Abid, N. (2023). Enhanced IoT network security with machine learning techniques for anomaly detection and classification. *Int. J. Curr. Eng. Technol*, *13*(6), 536-44.

Abraham, D., Toftegaard, Ø., DR, B. B. J., Gebremedhin, A., & Yildirim Yayilgan, S. (2024). Consequence simulation of cyber attacks on key smart grid business cases. *Frontiers in Energy Research*, *12*, 1395954.

Abusitta, A., de Carvalho, G. H., Wahab, O. A., Halabi, T., Fung, B. C., & Al Mamoori, S. (2023). Deep learning-enabled anomaly detection for IoT systems. *Internet of Things*, *21*, 100656.

Abu-Tair, M., Ali, A., Gebresilassie, S. K., Rafferty, J., & Cui, Z. (2024, April). Regulation Compliance System for IoT Environments: GDPR Compliance as a Use-Case. In *International Conference on Advanced Information Networking and Applications* (pp. 147-160). Cham: Springer Nature Switzerland.

Addison, S. K., Tahir, M., & Isoaho, J. (2025). Experimental Implementation of a Low Cost Real-Time Threat Intelligence Solution for Smart Home Security. *Procedia Computer Science*, *257*, 575-582.

Adhikary, A., Halder, S., Bose, R., Panja, S., Halder, S., Pratihar, J., & Dey, A. (2024). Design and implementation of an iot-based smart home automation system in real world scenario. *EAI Endorsed Transactions on Internet of Things*, *10*, 1-8.

Ahamed, S. I., Haque, M. M., & Asif, K. I. (2007, April). S-MARKS: A middleware secure by design for the pervasive computing environment. In *Fourth International Conference on Information Technology (ITNG'07)* (pp. 303-310). IEEE.

Aiello, M. (2022). IoT architectures: from data to smart systems. *Frontiers in the Internet of Things*, *1*, 959268.

Albany, M., Alsahafi, E., Alruwili, I., & Elkhediri, S. (2022). A review: Secure Internet of thing System for Smart Houses. *ANT/EDI40*, 437-444.

Albayaydh, W., Flechais, I., Zhao, R., & Albayaydh, J. (2025). AI For Privacy in Smart Homes: Exploring How Leveraging AI-Powered Smart Devices Enhances Privacy Protection. *arXiv preprint arXiv:2509.14050*.

Aldahmani, A., Ouni, B., Lestable, T., & Debbah, M. (2023). Cyber-security of embedded IoTs in smart homes: challenges, requirements, countermeasures, and trends. *IEEE Open Journal of Vehicular Technology*, *4*, 281-292.

Alharbi, R., & Aspinall, D. (2018, March). An IoT analysis framework: An investigation of IoT smart cameras' vulnerabilities. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-10). IET.

Ali, A. (2022, July). *Securing IoT connectivity: The role of Multi-Factor Authentication (MFA) in strengthening Cyber defense*.

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors*, *18*(3), 817.

Alicia. (2024, June 26). *Matter vs. Zigbee: Exploring the differences*. Reolink Blog. https://reolink.com/blog/matter-vs-zigbee/

Alpandinar, E. (2024). Constitutional Symmetry and Divergence: Louisiana's Fourth Amendment Analog Provides More Protection than the Federal Fourth Amendment for Technological Communications of Data. *LSU J. Energy L. & Resources*, *12*, 179.

Alraja, M. N., Farooque, M. M. J., & Khashab, B. (2019). The effect of security, privacy, familiarity, and trust on users' attitudes toward the use of the IoT-based healthcare: the mediation role of risk perception. *Ieee Access*, *7*, 111341-111354.

Alsalman, D. (2024). A comparative study of anomaly detection techniques for IoT security using adaptive machine learning for IoT threats. *IEEE Access*, *12*, 14719-14730.

Altaie, Rusul & Sahib, Rihab & Hamoud Hamza, Aseel & Hussein, Ghadeer. (2025). Hybrid Lightweight Encryption Algorithms for Internet of Things (IoT). 13. 33-39. 10.25673/121718.

Altulaihan, E., Almaiah, M. A., & Aljughaiman, A. (2024). Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms. *Sensors*, *24*(2), 713.

Ang, S., Ho, M., Huy, S., & Janarthanan, M. (2025). Utilizing IDS and IPS to improve cybersecurity monitoring process. *Journal of Cyber Security and Risk Auditing*, *2025*(3), 77-88.

Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. *IEEE Internet of Things Journal*, *6*(5), 9042-9053.

Apthorpe, N., Reisman, D., & Feamster, N. (2017). A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805*.

Arar, M., Jung, C., Awad, J., & Chohan, A. H. (2021). Analysis of smart home technology acceptance and preference for elderly in Dubai, UAE. *Designs*, *5*(4), 70.

Asghar, I., Khan, M. A., Ahmad, T., Ullah, S., Mansoor ul Hassan, K., & Buriro, A. (2023). Fortifying smart home security: A robust and efficient user-authentication scheme to counter node capture attacks. *Sensors*, *23*(16), 7268.

Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., & Olaniyi, O. O. (2024). Evaluating the trade-offs between wireless security and performance in IoT networks: A case study of web applications in AI-driven home appliances. *Available at SSRN 4927991*.

Babun, L., Aksu, H., Ryan, L., Akkaya, K., Bentley, E. S., & Uluagac, A. S. (2020, June). Z-iot: Passive device-class fingerprinting of zigbee and z-wave iot devices. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-7). IEEE.

Barbosa, N. M., Park, J. S., Yao, Y., & Wang, Y. (2019). "What if?" Predicting individual users' smart home privacy preferences and their changes. *Proceedings on Privacy Enhancing Technologies*.

Barbosa, N. M., Zhang, Z., & Wang, Y. (2020). Do privacy and security matter to everyone? quantifying and clustering {User-Centric} considerations about smart home device adoption. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (pp. 417-435).

Batalla, J. M., Vasilakos, A., & Gajewski, M. (2017). Secure smart homes: Opportunities and challenges. *ACM Computing Surveys (CSUR)*, *50*(5), 1-32.

Bathalapalli, V. K., Mohanty, S. P., Pan, C., & Kougianos, E. (2025). Qpuf: Quantum physical unclonable functions for security-by-design of industrial internet-of-things. *Cryptography*, *9*(2), 34.

Bazzi, H., Nassar, A., & Bizri, M. (2024). A Practical Intrusion Detection Approach For Arp Spoofing And Mitm In Local Area Networks. *BAU Journal-Science and Technology*, *6*(1), 10.

Bentotahewa, V., Yousif, M., Hewage, C., Nawaf, L., & Williams, J. (2022). Privacy and security challenges and opportunities for IoT technologies during and beyond COVID-19. *Privacy, Security And Forensics in The Internet of Things (IoT)*, 51-76.

Bhardwaj, A., Kaushik, K., Bharany, S., & Kim, S. (2023). Forensic analysis and security assessment of IoT camera firmware for smart homes. *Egyptian Informatics Journal*, *24*(4), 100409.

Bhardwaj, I., Kumar, A., & Bansal, M. (2017, September). A review on lightweight cryptography algorithms for data security and authentication in IoTs. In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 504-509). IEEE.

Birchley, G., Huxtable, R., Murtagh, M., Ter Meulen, R., Flach, P., & Gooberman-Hill, R. (2017). Smart homes, private homes? An empirical study of technology researchers' perceptions of ethical issues in developing smart-home health technologies. *BMC medical ethics*, *18*(1), 23.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016, August). On privacy and security challenges in smart connected homes. In *2016 European intelligence and security informatics conference (EISIC)* (pp. 172-175). IEEE.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2021). PRASH: a framework for privacy risk analysis of smart homes. *Sensors*, *21*(19), 6399.

Bureau Veritas Cybersecurity. (n.d.). *IoT products required to meet minimum security standards starting 2024*. Bureau Veritas. Διαθέσιμο στο: https://www.bureauveritas.com/newsroom/iot-products-required-meet-minimum-security-standards-starting-2024 Ανάκτηση στις 26/11/2025.

Burhan, M., Rehman, R. A., Khan, B., & Kim, B. S. (2018). IoT elements, layered architectures and security issues: A comprehensive survey. *sensors*, *18*(9), 2796.

Butt, U., shaheer Gutappa, B., Pendlebury, G., Hassan, B., Butt, W., & Davelis, A. (2023). IoT privacy by design. In *Opportunities and Challenges of Business 5.0 in Emerging Markets* (pp. 270-300). IGI Global.

Caballero-Gil, C., Alvarez, R., Hernández-Goya, C., & Molina-Gil, J. (2024). Research on smart-locks cybersecurity and vulnerabilities. *Wireless Networks*, *30*(6), 5905-5917.

Cawley, C. (2024, May 27). *Matter vs Z-Wave: What's the difference?* Matter Alpha. Διαθέσιμο στο: https://www.matteralpha.com/explainer/matter-vs-zwave-whats-the-difference Ανάκτηση στις 24/11/2025.

Cecílio, J., & Souto, A. (2024, May). Security issues in industrial Internet-of-Things: Threats, attacks and solutions. In *2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4. 0 & IoT)* (pp. 458-463). IEEE.

Chalhoub, G., Kraemer, M. J., Nthala, N., & Flechais, I. (2021, May). "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI conference on human factors in computing systems* (pp. 1-16).

Cherian, M. M., & Varma, S. L. (2022). Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks. *International Journal of Computer Network and Information Security*, *15*(1), 52.

Chhetri, C., & Genaro Motti, V. (2022). User-centric privacy controls for smart homes. *Proceedings of the ACM on Human-Computer Interaction*, *6*(CSCW2), 1-36.

Chhetri, C., & Motti, V. (2020). Identifying vulnerabilities in security and privacy of smart home devices. In *National Cyber Summit* (pp. 211-231). Cham: Springer International Publishing.

Chiba, Z., Abghour, N., Moussaid, K., Lifandali, O., & Kinta, R. (2022). A deep study of novel intrusion detection systems and intrusion prevention systems for Internet of Things networks. *Procedia Computer Science*, *210*, 94-103.

Choi, B. (2023). Verification of Technology Acceptance Model (TAM) Research Model Applied to Smart Home for College Students-An Analysis of Acceptability Diagnosis and its Influence Factors for Smart Homes in S. Korea. *Journal of the Korean Housing Association*, *34*(6), 081-092.

Choudhary, Y., Umamaheswari, B., & Kumawat, V. (2021). A study of threats, vulnerabilities and countermeasures: An iot perspective. *Humanities*, *8*(4), 39-45.

Cimperman, M., Brenčič, M. M., & Trkman, P. (2016). Analyzing older users' home telehealth services acceptance behavior—applying an Extended UTAUT model. *International journal of medical informatics*, *90*, 22-31.

Coston, I., Plotnizky, E., & Nojoumian, M. (2025). Comprehensive Study of IoT Vulnerabilities and Countermeasures. *Applied Sciences*, *15*(6), 3036.

Coulibaly, K. (2020). An overview of intrusion detection and prevention systems. *arXiv preprint arXiv:2004.08967*.

Dąbrowska, M. (2024, July 30). *The power of IoT home automation*. IoT Now. Διαθέσιμο στο: https://www.iot-now.com/2024/07/30/145721-the-power-of-iot-home-automation/ Ανάκτηση στις 22/11/2025.

Danbatta, S. J., & Varol, A. (2019, June). Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE.

Dasgupta, A., Gill, A. Q., & Hussain, F. (2019). Privacy of IoT-enabled smart home systems. *Internet of Things (IoT) for automated and smart applications*, 9.

Davis, B. D., Mason, J. C., & Anwar, M. (2020). Vulnerability studies and security postures of IoT devices: A smart home case study. *IEEE Internet of Things Journal*, *7*(10), 10102-10110.

Del-Real, C., De Busser, E., & van den Berg, B. (2024). Shielding software systems: A comparison of security by design and privacy by design based on a systematic literature review. *Computer Law & Security Review*, *52*, 105933.

Del-Real, C., De Busser, E., & van den Berg, B. (2025). A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies. *International Review of Law, Computers & Technology*, 1-32.

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications*, *112*(3), 1947-1980.

Dhanraj, T., Kumar, M., Singh, S., Kumar, R., Jaiswal, P., & Mohapatra, H. (2024). A review on mitigating privacy risks in IoT-enabled smart homes. *Computer networks and communications*, 132-147.

Dilraj, M., Nimmy, K., & Sankaran, S. (2019, October). Towards behavioral profiling based anomaly detection for smart homes. In *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)* (pp. 1258-1263). IEEE.

Ding, Z., He, D., Qiao, Q., Li, X., Gao, Y., Chan, S., & Choo, K. K. R. (2023). A lightweight and secure communication protocol for the IoT environment. *IEEE Transactions on Dependable and Secure Computing*, *21*(3), 1050-1067.

Diro, A., Chilamkurti, N., Nguyen, V. D., & Heyne, W. (2021). A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. *Sensors*, *21*(24), 8320.

Distler, V., Lallemand, C., & Koenig, V. (2020). How acceptable is this? How user experience factors can broaden our understanding of the acceptance of privacy trade-offs. *Computers in Human Behavior*, *106*, 106227.

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Dusun IoT. (2024, January 18). *Smart home hub, all you need to know in 2024*. Dusuniot. Διαθέσιμο στο: https://www.dusuniot.com/blog/smart-home-hub-all-you-need-to-know-in-2023/ Ανάκτηση στις 28/12/2025.

Elmarkez, A., Mesli-Kesraoui, S., Berruet, P., & Oquendo, F. (2025). Security by Design for Industrial Control Systems from a Cyber–Physical System Perspective: A Systematic Mapping Study. *Machines*, *13*(7), 538.

EpiSensor. (2024). *IoT data privacy: Ensuring compliance with GDPR and other regulations*. Episensor Knowledge Base. Διαθέσιμο στο: https://episensor.com/knowledge-base/iot-data-privacy-ensuring-compliance-with-gdpr-and-other-regulations/ Ανάκτηση στις 24/11/2025.

Eskandari, M., Janjua, Z. H., Vecchio, M., & Antonelli, F. (2020). Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, *7*(8), 6882-6897.

Ezugwu, A. E., Taiwo, O., Egwuche, O. S., Abualigah, L., Van Der Merwe, A., Pal, J., ... & Olusanya, M. O. (2025). Smart Homes of the Future. *Transactions on Emerging Telecommunications Technologies*, *36*(1), e70041.

Farooq, M., & Hassan, M. (2021). IoT smart homes security challenges and solution. *International Journal of Security and Networks*, *16*(4), 235-243.

Fereidouni, H., Fadeitcheva, O., & Zalai, M. (2025). IoT and man-in-the-middle attacks. *Security and Privacy*, *8*(2), e70016.

Fernandes, E., Jung, J., & Prakash, A. (2016, May). Security analysis of emerging smart home applications. In *2016 IEEE symposium on security and privacy (SP)* (pp. 636-654). IEEE.

Garg, A. (2022). Behavioral biometrics for IoT security: A machine learning framework for smart homes. *Journal of Recent Trends in Computer Science and Engineering*, *10*(2), 71-92.

Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017, May). Security and privacy issues for an IoT based smart home. In *2017 40th*

international convention on information and communication technology, electronics and microelectronics (MIPRO) (pp. 1292-1297). IEEE.

Ghazali, T. K., & Zakaria, N. H. (2018). Security, comfort, healthcare, and energy saving: A review on biometric factors for smart home environment. *Journal of Computers*, *29*(1), 189-208

Gillis, A. S., Hashemi-Pour, C., & Wigmore, I. (2025, July 23). *What is Internet of Things privacy (IoT privacy)?* Διαθέσιμο στο: TechTarget. https://www.techtarget.com/searchiot/definition/internet-of-things-privacy-IoT-privacy Ανάκτηση στις 12/11/2025.

Goyal, T. K., Sahula, V., & Kumawat, D. (2022). Energy efficient lightweight cryptography algorithms for IoT devices. *IETE Journal of Research*, *68*(3), 1722-1735.

Grand View Research. (2024). *IoT devices market (2025–2030): Size, share & trends analysis report*. Διαθέσιμο στο: https://www.grandviewresearch.com/industry-analysis/iot-devices-market-report Ανάκτηση στις 21/11/2025.

Grand View Research. (2025). *U.S. smart home market (2025–2030): Size, share & trends analysis report*. Διαθέσιμο στο: https://www.grandviewresearch.com/industry-analysis/us-smart-home-market-report Ανάκτηση στις

Grünewald, P., & Reisch, T. (2020). The trust gap: Social perceptions of privacy data for energy services in the United Kingdom. *Energy Research & Social Science*, *68*, 101534.

Gu, W., Bao, P., Hao, W., & Kim, J. (2019). Empirical examination of intention to continue to use smart home services. *Sustainability*, *11*(19), 5213.

Gudala, L., Shaik, M., Venkataramanan, S., & Sadhu, A. K. R. (2019). Leveraging artificial intelligence for enhanced threat detection, response, and anomaly identification in resource-constrained iot networks. *Distributed Learning and Broad Applications in Scientific Research*, *5*, 23-54.

Guhr, N., Werth, O., Blacha, P. P. H., & Breitner, M. H. (2020). Privacy concerns in the smart home context. *SN Applied Sciences*, *2*(2), 247.

Gunathilake, N. A., Buchanan, W. J., & Asif, R. (2019, April). Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 707-710). IEEE.

Gupta, N., Jindal, V., & Bedi, P. (2023). A survey on intrusion detection and prevention systems. *SN Computer Science*, *4*(5), 439.

Hammoudeh, M., & Arioua, M. (2018). Sensors and actuators in Smart Cities. *Journal of Sensor and Actuator Networks*, *7*(1), 8.

Haris, M. A. H. B., Yahya, M. I. H. B., & Ibrahim, M. N. B. (2023). Security and Privacy Issues in Internet of Things (IoT). *Authorea Preprints*.

Harvey, P., Toutsop, O., Kornegay, K., Alale, E., & Reaves, D. (2020, December). Security and privacy of medical internet of things devices for smart homes. In *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)* (pp. 1-6). IEEE.

Hazazi, H. (2024). *Understanding and Improving the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User* (Doctoral dissertation, The University of North Carolina at Charlotte).

Huijts, N. M., Haans, A., Budimir, S., Fontaine, J. R., Loukas, G., Bezemskij, A., ... & Roesch, E. B. (2023). User experiences with simulated cyber-physical attacks on smart home IoT. *Personal and Ubiquitous Computing*, *27*(6), 2243-2266.

IEEE BLP. (2024). *What is an actuator in IoT?* Διαθέσιμο στο: https://blp.ieee.org/what-is-actuator-in-iot/ Ανάκτηση στις 18/11/2025.

Integrated Media Systems. (2024, August 31). *Privacy and security in smart homes: Keeping your digital sanctuary safe*. IMSVA. Διαθέσιμο στο: https://www.imsva.com/blog/2024/august/privacy-and-security-in-smart-homes-keeping-your/ Ανάκτηση στις 25/11/2025.

Intuz. (2024, July 11). *What is the Matter protocol and how does it work?* Διαθέσιμο στο: https://www.intuz.com/blog/what-is-the-matter-protocol-and-how-does-it-work Ανάκτηση στις 20/11/2025.

Jacobsson, A., & Davidsson, P. (2015, December). Towards a model of privacy and security for smart homes. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 727-732). IEEE.

Jahid, M. S. R. (2025). AI-Powered Smart Home Automation: Enhancing Security, Energy Efficiency, And User Experience In Modern Housing. *American Journal of Interdisciplinary Studies*, *6*(02), 76-114.

Jangam, S. K., & Muntala, P. S. R. P. (2022). Role of Artificial Intelligence and Machine Learning in IoT Device Security. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *3*(1), 77-86.

Jayalaxmi, P. L. S., Saha, R., Kumar, G., Conti, M., & Kim, T. H. (2022). Machine and deep learning solutions for intrusion detection and prevention in IoTs: A survey. *IEEe Access*, *10*, 121173-121192.

Jeffrey, N., Tan, Q., & Villar, J. R. (2023, August). Intrusion detection and prevention in industrial internet of things: A study. In *Computational Intelligence in Security for Information Systems Conference* (pp. 37-48). Cham: Springer Nature Switzerland.

Jhuang, Y. Y., Yan, Y. H., & Horng, G. J. (2023). GDPR personal privacy security mechanism for smart home system. *Electronics*, *12*(4), 831.

Jøsang, A. (2024). Secure by Design. In *Cybersecurity: Technology and Governance* (pp. 243-270). Cham: Springer Nature Switzerland.

Jose, A. C., & Malekian, R. (2017). Improving smart home security: Integrating logical sensing into smart home. *IEEE Sensors Journal*, *17*(13), 4269-4286.

Kairaldeen, A. R., Abdullah, N. F., Abu-Samah, A., & Nordin, R. (2021). Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms. *Wireless Communications and Mobile Computing*, *2021*(1), 4401809.

Kang, H. J., Han, J., & Kwon, G. H. (2022). The acceptance behavior of smart home health care services in South Korea: an integrated model of UTAUT and TTF. *International Journal of Environmental Research and Public Health*, *19*(20), 13279.

Kennedy, M. R., Huxtable, R., Birchley, G., Ives, J., & Craddock, I. (2021). "A Question of Trust" and "a Leap of Faith"—Study Participants' Perspectives on Consent, Privacy, and Trust in Smart Home Research: Qualitative Study. *JMIR mHealth and uHealth*, *9*(11), e25227.

Khan, H. U., Alomari, M. K., Khan, S., Nazir, S., Gill, A. Q., Al-Maadid, A. A., ... & Hassan, M. K. (2021). Systematic analysis of safety and security risks in smart homes.

Khan, M. M., & Alkhathami, M. (2024). Anomaly detection in IoT-based healthcare: machine learning for enhanced security. *Scientific Reports*, *14*(1), 5872.

Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. *IEEE Internet of Things Journal*, *8*(6), 4132-4156.

Khashan, O. A., Ahmad, R., & Khafajah, N. M. (2021). An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks. *Ad Hoc Networks*, *115*, 102448.

Khoa, T. A., Nhu, L. M. B., Son, H. H., Trong, N. M., Phuc, C. H., Phuong, N. T. H., ... & Duc, D. N. M. (2020). Designing efficient smart home management with IoT smart lighting: a case study. *Wireless communications and mobile computing*, *2020*(1), 8896637.

Kohli, R., Gupta, S., & Gaur, M. S. (2025). Guarding Digital Privacy: Exploring User Profiling and Security Enhancements. *arXiv preprint arXiv:2504.07107*.

Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, *16*(4), 1933-1954.

Kraemer, M. J., & Flechais, I. (2018, March). Researching privacy in smart homes: A roadmap of future directions and research methods. In *Living in the Internet of Things: Cybersecurity of the IoT-2018* (pp. 1-10). IET.

Kulyk, O., Milanovic, K., & Pitt, J. (2020, October). Does my smart device provider care about my privacy? Investigating trust factors and user attitudes in IoT systems. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (pp. 1-12).

Kumar, A., Abhishek, K., Ghalib, M. R., Shankar, A., & Cheng, X. (2022). Intrusion detection and prevention system for an IoT environment. *Digital Communications and Networks*, *8*(4), 540-551.

Kumar, D., Pawar, P. P., Addula, S. R., Meesala, M. K., Oni, O., Cheema, Q. N., ... & Sajja, G. S. (2025). AI-Powered security for IoT ecosystems: a hybrid deep learning approach to anomaly detection. *Journal of Cybersecurity and Privacy*, *5*(4), 90.

Kumar, P. (2025). Next-generation secure authentication and access control architectures: advanced techniques for securing distributed systems in modern enterprises. *International Journal of Computational and Experimental Science and ENgineering (IJCESEN) Vol*, 4966-4995.

Lee, C., Zappaterra, L., Choi, K., & Choi, H. A. (2014, October). Securing smart home: Technologies, security challenges, and security requirements. In *2014 IEEE Conference on Communications and Network Security* (pp. 67-72). IEEE.

Li, J., Sun, K., Huff, B. S., Bierley, A. M., Kim, Y., Schaub, F., & Fawaz, K. (2023, May). "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 2850-2866). IEEE.

Lilian, J. (2024). Determinants of Smart Home Products Adoption: Based on the Technology Acceptance Model. *Journal of Management and Humanity Research*, *12*, 1-24.

Lipps, C., Herbst, J., & Schotten, H. D. (2021, February). How to Dance Your Passwords: A Biometric MFA-Scheme for Identification and Authentication of

Individuals in IIoT Environments. In *ICCWS 2021 16th International Conference on Cyber Warfare and Security* (p. 168). Academic Conferences Limited.

Liu, Y., Gan, Y., Song, Y., & Liu, J. (2021). What influences the perceived trust of a voice-enabled smart home system: an empirical study. *Sensors*, *21*(6), 2037.

Lopez, N. A. T., Pasaoa, J. R. B., Parado, J. A., & Morales, J. O. (2016). A comparative study of thread against zigbee, z-wave, bluetooth, and wi-fi as a home-automation networking protocol. *Research Proposal*.

Luo, Y., Cheng, L., Hu, H., Peng, G., & Yao, D. (2020). Context-rich privacy leakage analysis through inferring apps in smart home iot. *IEEE Internet of Things Journal*, *8*(4), 2736-2750.

Magara, T., & Zhou, Y. (2024). Internet of things (IoT) of smart homes: privacy and security. *Journal of Electrical and Computer Engineering*, *2024*(1), 7716956.

Mamonov, S., & Benbunan-Fich, R. (2021). Unlocking the smart home: exploring key factors affecting the smart lock adoption intention. *Information Technology & People*, *34*(2), 835-861.

Marchang, J., McDonald, J., Keishing, S., Zoughalian, K., Mawanda, R., Delhon-Bugard, C., & Bouillet, N. (2024). Secure by Design Real-Time IoMT Architecture for e-Health Population Monitoring (RTPM).

Mariappan, K., Ganesan, P., & Jagatheesaperumal, S. K. (2025). IoT access control and authentication schemes. In *Internet of Things Security* (pp. 87-106). Elsevier.

MarketsandMarkets. (2024, October 21). *Smart home market research report: 2024 overview*. Διαθέσιμο στο: https://www.marketsandmarkets.com/ResearchInsight/smart-home-market-research.asp Ανάκτηση στις 22/11/2025.

Mashal, I., Shuhaiber, A., & Al-Khatib, A. W. (2023). User acceptance and adoption of smart homes: A decade long systematic literature review. *International Journal of Data and Network Science*, *7*(2), 533.

Meixiu, L., & Wenhao, Z. (2025). Developing a Context-Aware Intrusion Detection Model for Smart Home Environments Integrating Behavioral Biometrics and Device Profiling. *Chronicle of Emerging Scientific Paradigms*, *15*(5), 1-16.

Mendes, T. D., Godina, R., Rodrigues, E. M., Matias, J. C., & Catalão, J. P. (2015). Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. *Energies*, *8*(7), 7279-7311.

Mocrii, D., Chen, Y., & Musilek, P. (2018). IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet of Things*, *1*, 81-98.

Möller, D. P. (2023). Intrusion detection and prevention. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 131-179). Cham: Springer Nature Switzerland.

Mosenia, A., Sur-Kolay, S., Raghunathan, A., & Jha, N. K. (2017). DISASTER: dedicated intelligent security attacks on sensor-triggered emergency responses. *IEEE Transactions on Multi-Scale Computing Systems*, *3*(4), 255-268.

Mothukuri, V., Khare, P., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Srivastava, G. (2021). Federated-learning-based anomaly detection for IoT security attacks. *IEEE Internet of Things Journal*, *9*(4), 2545-2554.

Muthusamy, A., & Sakthi, G. (2025). Multifactor Authentication (MFA), the Golden Lock for Cloud Entry: By Adopting MFA, Organizations and Individuals Can Significantly Reduce the Risk of Security Breach. In *Risk-Based Approach to Secure Cloud Migration* (pp. 285-300). IGI Global Scientific Publishing.

Naidu, G. A., & Kumar, J. (2019). Wireless protocols: Wi-fi son, bluetooth, zigbee, z-wave, and wi-fi. In *Innovations in Electronics and Communication Engineering: Proceedings of the 7th ICIECE 2018* (pp. 229-239). Singapore: Springer Singapore.

Naru, E. R., Saini, H., & Sharma, M. (2017, February). A recent review on lightweight cryptography in IoT. In *2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC)* (pp. 887-890). IEEE.

Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014, October). An experimental study of security and privacy risks with emerging household appliances. In *2014 IEEE conference on communications and network security* (pp. 79-84). IEEE.

Orlowski, A., & Loh, W. (2025). Data autonomy and privacy in the smart home: the case for a privacy smart home meta-assistant. *AI & SOCIETY*, 1-14.

Pal, D., Funilkul, S., Vanijja, V., & Papasratorn, B. (2018). Analyzing the elderly users' adoption of smart-home services. *IEEE access*, *6*, 51238-51252.

Park, H., Basaran, C., Park, T., & Son, S. H. (2014). Energy-efficient privacy protection for smart home environments using behavioral semantics. *Sensors*, *14*(9), 16235-16257.

Park, M., Oh, H., & Lee, K. (2019). Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective. *Sensors*, *19*(9), 2148.

Patterson, B. (2025, September 23). *I'm a smart home expert: These are the smart devices I can't live without*. PCWorld. Διαθέσιμο στο: https://www.pcworld.com/article/2606839/im-a-smart-home-expert-these-are-the-smart-devices-i-cant-live-without.html Ανάκτηση στις 23/11/2025.

Percy-Campbell, J., Buchan, J., Chu, C. H., Bianchi, A., Hoey, J., & Khan, S. S. (2024). User Perception of Smart Home Surveillance: An Integrative Review. *Surveillance & Society*, *22*(3), 304-324.

Piasecki, S. (2023). Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons. *Information & Communications Technology Law*, *32*(3), 385-417.

Pierce, J. (2019, May). Smart home security cameras and shifting lines of creepiness: A design-led inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).

Prajapati, P., Bhatt, B., Zalavadiya, G., Ajwalia, M., & Shah, P. (2021, January). A review on recent intrusion detection systems and intrusion prevention systems in

IoT. In *2021 11th International conference on cloud computing, data science & engineering (Confluence)* (pp. 588-593). IEEE.

Prashanth, J. S., Krishna, G. B., Prasad, A. V., & Rao, P. R. (2025, March). Smart Farming Revolution: A Cutting-Edge Review of Deep Learning and IoT Innovations in Agriculture. In *Operations Research Forum* (Vol. 6, No. 1, pp. 1-39). Springer International Publishing.

Protick, T. I., Sabir, A., Abhinaya, S., Bartlett, A., & Das, A. (2024). Unveiling Users' Security and Privacy Concerns Regarding Smart Home IoT Products from Online Reviews. *ACM Journal on Computing and Sustainable Societies*, *2*(4), 1-41.

Puentes-Conde, G. M., Sifuentes, E., Molina, J., Enríquez-Aguilera, F., Bravo, G., & Enríquez, G. N. (2025). Direct Interface Circuits for Resistive, Capacitive, and Inductive Sensors: A Review. *Electronics*, *14*(12), 2393.

Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends. *Sensors*, *24*(6), 1968.

Rahman, M. M., Gupta, D., Bhatt, S., Shokouhmand, S., & Faezipour, M. (2024). A comprehensive review of machine learning approaches for anomaly detection in smart homes: experimental analysis and future directions. *Future Internet*, *16*(4), 139.

Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S. (2019, October). Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In *2019 International Carnahan Conference on Security Technology (ICCST)* (pp. 1-6). IEEE.

Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, *129*, 77-89.

Rao, U. H., & Nayak, U. (2014). Intrusion detection and prevention systems. In *The InfoSec handbook: an introduction to information security* (pp. 225-243). Berkeley, CA: Apress.

Regmi, X. Z., NEAL, T., RUIZ, J., & ANTHONY, L. (2025). 'Over Time Everyone's Gonna Be Open to It': User Attitudes Toward Security and Privacy in Continuous Authentication for Smart Homes.

Reichherzer, T., Mishra, A., Kalaimannan, E., & Wilde, N. (2016, December). A case study on the trade-offs between security, scalability, and efficiency in smart home sensor networks. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 222-225). IEEE.

Renu, S. (2019). Security & Privacy Challenges in Smart Home. International Journal of Engineering and Advanced Technology. 8. 3169-3171. 10.35940/ijeat.F9268.088619.

Salimon, M. G., Goronduste, H. A., & Abdullah, H. (2018). User adoption of Smart Homes Technology in Malaysia: Integration TAM 3, TPB, UTAUT 2 and extension of their constructs for a better prediction. *IOSR Journal of Business and Management*, *20*(4), 60-69.

Sanchez, I., Satta, R., Fovino, I. N., Baldini, G., Steri, G., Shaw, D., & Ciardulli, A. (2014, October). Privacy leakages in smart home wireless technologies. In *2014 international carnahan conference on security technology (ICCST)* (pp. 1-6). IEEE.

Schomakers, E. M., Biermann, H., & Ziefle, M. (2020, July). Understanding privacy and trust in smart home environments. In *International Conference on Human-Computer Interaction* (pp. 513-532). Cham: Springer International Publishing.

Schulz, J. M., & Scilla, J. S. (2024). Broad Perspective of Smart Home Technology in 2024. *International Journal of Smart Technologies (IJST)*, *1*(1), 1-27.

Shahidi, H. (2019). Security Challenges of Communication Protocols in IoT: Comparing security features of ZigBee and Z-Wave communication protocols in IoT devices.

Sharma, A., Sangal, A. L., & Sharma, K. C. (2025). Privacy-Preserving Prosumer Profiling using Smart Meter Data. *Sustainable Energy, Grids and Networks*, 101784.

Shouran, Z., Ashari, A., & Priyambodo, T. (2019). Internet of things (IoT) of smart home: privacy and security. *International Journal of Computer Applications*, *182*(39), 3-8.

Shuhaiber, A., & Mashal, I. (2019). Understanding users' acceptance of smart homes. *Technology in society*, *58*, 101110.

Shukla, S., Varshney, G., Singh, S., & Goel, S. (2025). A passwordless MFA utilizing biometrics, proximity, and contactless communication. *Information Security Journal: A Global Perspective*, *34*(6), 633-654.

Sikdar, D. (2024, July 11). *Matter vs Z-Wave: What you need to know*. Silicon Labs Blog. Διαθέσιμο στο: https://www.silabs.com/blog/matter-vs-z-wave-what-you-need-to-know Ανάκτηση στις 25/11/2025.

Singh, D., Psychoula, I., Kropf, J., Hanke, S., & Holzinger, A. (2018, June). Users' perceptions and attitudes towards smart home technologies. In *International Conference on smart homes and Health Telematics* (pp. 203-214). Cham: Springer International Publishing.

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, *15*(2), 1625-1642.

Sivanathan, A., Loi, F., Gharakheili, H. H., & Sivaraman, V. (2017, December). Experimental evaluation of cybersecurity threats to the smart-home. In *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1-6). IEEE.

Sivaraman, V., Gharakheili, H. H., Fernandes, C., Clark, N., & Karliychuk, T. (2018). Smart IoT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine*, *37*(2), 71-79.

Sokol, I., Hubinský, P., & Chovanec, Ľ. (2021). Lightweight cryptography for the encryption of data communication of iot devices. *Electronics*, *10*(21), 2567.

Stolojescu-Crisan, C., Crisan, C., & Butunoi, B. P. (2021). An IoT-based smart home automation system. *Sensors*, *21*(11), 3784.

Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital health*, *9*, 20552076231177144.

Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2024). A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *IEEE Access*, *12*, 23096-23121.

Tyagi, V., Saraswat, A., & Bansal, S. (2023). An analysis of securing Internet of Things (IoT) devices from man-in-the-middle (MIMA) and denial of service (DoS). In *Smart Cities* (pp. 337-357). CRC Press.

Tyagi, V., Saraswat, A., Kumar, A., & Gambhir, S. (2024). Securing IoT Devices Against MITM and DoS Attacks: An Analysis. *Reshaping Intelligent Business and Industry: Convergence of AI and IoT at the Cutting Edge*, 237-249.

Ullah, I., & Mahmoud, Q. H. (2021). Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEe Access*, *9*, 103906-103926.

Valencia-Arias, A., Cardona-Acevedo, S., Gomez-Molina, S., Gonzalez-Ruiz, J. D., & Valencia, J. (2023). Smart home adoption factors: A systematic literature review and research agenda. *Plos one*, *18*(10), e0292558.

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the internet of things. *Electronics*, *13*(16), 3343.

Varol, A. B. (2019, September). Compilation of data link protocols: Bluetooth low energy (ble), zigbee and z-wave. In *2019 4th International Conference on Computer Science and Engineering (UBMK)* (pp. 85-90). IEEE.

Varri, D. B. S. (2021). Cloud-Native Security Architecture for Hybrid Healthcare Infrastructure. *Available at SSRN 5785982*.

Vattheuer, C., Liu, C., Abedi, A., & Abari, O. (2023). Is z-wave reliable for iot sensors?. *IEEE Sensors Journal*, *23*(24), 31297-31306.

Wajid, S., & Sans, M. (2024). Internet of Things Security: Leveraging AI and Machine Learning for Anomaly Detection.

Wang, H., Chen, Y. P., Bista, D., Calvo, R., Regmi, N., Zhang, X., ... & Anthony, L. (2025). 'Over Time Everyone's Gonna Be Open To It': User Attitudes Towards Security and Privacy in Continuous Authentication for Smart Homes. *IEEE Access*.

Wang, M., Yang, N., & Weng, N. (2023). Securing a smart home with a transformer-based IoT intrusion detection system. *Electronics*, *12*(9), 2100.

Wolniak, R. (2024). The usage of smart locks in smart home. Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska.

Xenofontos, C., Zografopoulos, I., Konstantinou, C., Jolfaei, A., Khan, M. K., & Choo, K. K. R. (2021). Consumer, commercial, and industrial iot (in) security: Attack taxonomy and case studies. *IEEE Internet of Things Journal*, *9*(1), 199-221.

Xu, R., Zeng, Q., Zhu, L., Chi, H., Du, X., & Guizani, M. (2019). Privacy leakage in smart homes and its mitigation: IFTTT as a case study. IEEE Access, 7, 63457-63471.

Yadav, R., & Kumar, V. (2022). Communication Security in IoT. In *Internet of Things: Security and Privacy in Cyberspace* (pp. 79-115). Singapore: Springer Nature Singapore.

Yao, Y., Basdeo, J. R., Mcdonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1-24.

Zeng, E., & Roesner, F. (2019). Understanding and improving security and privacy in {multi-user} smart homes: A design exploration and {in-home} user study. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 159-176).

Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 65-80).

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on human-computer interaction*, *2*(CSCW), 1-20.

Zhou, C., Qian, Y., & Kaner, J. (2024). A study on smart home use intention of elderly consumers based on technology acceptance models. *Plos one*, *19*(3), e0300574.

Zhraw, D. S., Hussain, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., & Aldarwish, A. J. (2025, April). Chronological Review of MITM Attacks: Challenges, Solutions and Recommendations. In *Computer Science On-line Conference* (pp. 202-220). Cham: Springer Nature Switzerland.

Zia, M. F., Siddiqua, M., Ouameur, M. A., Bagaa, M., & Al Turjman, F. (2025). Securing the Future: A Survey on Smart Home Security in IoT-Integrated Smart Cities.

Zou, Q., Li, Q., Li, R., Huang, Y., Tyson, G., Xiao, J., & Jiang, Y. (2023). Iotbeholder: A privacy snooping attack on user habitual behaviors from smart home wi-fi traffic. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, *7*(1), 1-26.