Smart-Home Security Using the Internet of Things

Threats and Countermeasures



By

George Vardakis

Department of Electrical and Computer
Engineering Hellenic Mediterranean
University

This dissertation is submitted for the
degree of *Doctor of Philosophy*

HELLENIC MEDITERRANEAN
UNIVERSITY DEPARTMENT OF
ELECTRICAL AND COMPUTER
ENGINEERING

DOCTORAL THESIS

Smart-Home Security

Using the Internet of Things

Threats and Countermeasures

Author: George Vardakis

Supervisors: Papadakis Nikos

Examiners:

A thesis submitted in fulfillment of the requirements for
the degree of Doctor of Philosophy

in the

Hellenic Mediterranean University

August, 2025

Declaration of Authorship

I, George Vardakis, declare that this thesis titled, “Smart-Home Security Using the Internet of Things, Threats and Countermeasures” and the work presented in it is my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.



Signed:

_____

Date: 01/08/2025

"Freedom would have no meaning without security in homes and streets"

Nelson Mandela

Acknowledgments

First and foremost, I would like to express my deepest gratitude to my supervisor, Assoc. Professor Papadakis Nikolaos. His patience, guidance, and unwavering support have been invaluable throughout my Ph.D. journey. His mentorship has been a constant source of motivation and I am incredibly grateful for the encouragement he has provided.

I am also indebted to my family for their boundless psychological support over the years. Especially, to my wife, Eleftheria, and my children, Catherine and Kostas, thank you for your steadfast love, understanding, and encouragement. Their belief in me has been a pillar of strength during the most challenging times.

This journey has been one of faith and perseverance, and I am forever thankful for the blessings that have made it possible.

Abstract

With the rapid advancements in the Internet of Things (IoT) landscape, the integration of interconnected devices within residential environments has catalyzed the widespread emergence of smart homes. While these developments facilitate enhanced interoperability and automation, they simultaneously introduce intricate security challenges stemming from device heterogeneity and the complexity of underlying communication protocols. This dissertation systematically maps the cybersecurity landscape of smart home ecosystems, advancing beyond generalized perspectives to provide an in-depth examination of critical IoT device categories including digital voice assistants, smart televisions, augmented and virtual reality systems (AR/VR), intelligent locks, and environmental sensors.

The study delineates representative threat vectors such as unauthorized system access, side-channel attacks, personal data exfiltration, firmware tampering, and device compromises. Furthermore, it critically evaluates current security mechanisms and methodologies designed to mitigate these risks, encompassing lightweight cryptographic protocols, multi-factor authentication (MFA) schemes, intrusion detection systems (IDS), and anomaly detection techniques, with the objective of fortifying system resilience against sophisticated adversarial behaviors.

Beyond the purely technical facets, this work underscores the pivotal role of user awareness and education in sustaining secure smart home environments. Despite technological improvements in construction standards and living conditions, subjective perceptions of safety remain frequently insufficient, prompting intensified research efforts towards advanced protective technologies. Heightened insecurity, particularly in densely populated urban centers, has stimulated the application of Artificial Intelligence (AI) and Machine Learning (ML) methods for the development of intelligent threat prevention and response systems, thereby enhancing both physical and cyber security perceptions.

Within this context, applications leveraging Deep Learning (DL) methodologies have emerged, transforming conventional residences into automated, adaptive, and secure infrastructures. The dissertation highlights DL’s dual contributions: enhancing

cybersecurity in smart homes and enabling interdisciplinary breakthroughs in domains such as medicine, where remarkable outcomes are observed. Detailed exposition is provided on the backpropagation algorithm employed in both linear and nonlinear artificial neural networks, including a case study of the XOR problem as a classical demonstration of nonlinearity.

Machine Learning demonstrates high efficacy in human activity analysis, particularly in facial recognition, which constitutes a foundational component for personalized management and security in smart home settings. The imperative for real-time processing of voluminous data, coupled with substantial computational demands, necessitates the deployment of fog and cloud computing paradigms to efficiently support image processing, face identification, and human silhouette recognition.

Collectively, these subsystems form a comprehensive security framework grounded in DL architectures and ML-trained models. Based on the findings of this research, it is substantiated that the application of such technologies significantly advances the realization of fully secure residences, addressing an urgent societal need especially in light of escalating crime rates.

Finally, the dissertation proposes avenues for future research aimed at further reinforcing IoT-enabled smart home security. Recommendations include the development of robust unified security standards, enhanced device authentication protocols, and the incorporation of intelligent intrusion detection mechanisms employing anomaly analytics and continuous learning. Addressing these technical challenges is essential for actualizing the vision of fully operational, secure, and threat-resilient IoT-enabled smart homes that safeguard user privacy and digital sovereignty.

Keywords: smart home, machine learning, deep learning, back propagation, neural networks, facial, silhouette and activities recognition, security, privacy, resilience.

Περίληψη

Με την ταχεία πρόοδο του Διαδικτύου των Πραγμάτων (IoT), η ενσωμάτωση διασυνδεδεμένων συσκευών στον οικιακό χώρο έχει προκαλέσει την ευρεία εξάπλωση των έξυπνων κατοικιών. Παρόλο που αυτές οι εξελίξεις διευκολύνουν την βελτιωμένη διαλειτουργικότητα και αυτοματοποίηση, παράλληλα εισάγουν σύνθετες προκλήσεις ασφαλείας, οι οποίες προκύπτουν από την ετερογένεια των συσκευών και την πολυπλοκότητα των υποκείμενων πρωτοκόλλων επικοινωνίας. Η παρούσα διατριβή χαρτογραφεί συστηματικά το τοπίο της κυβερνοασφάλειας στα οικοσυστήματα έξυπνου σπιτιού, προχωρώντας πέρα από γενικές προσεγγίσεις και προσφέροντας εις βάθος εξέταση κρίσιμων κατηγοριών IoT συσκευών, όπως οι ψηφιακοί φωνητικοί βοηθοί, οι έξυπνες τηλεοράσεις, τα συστήματα επαυξημένης και εικονικής πραγματικότητας (AR/VR), οι έξυπνες κλειδαριές και οι περιβαλλοντικοί αισθητήρες.

Η διατριβή αυτή, περιγράφει αντιπροσωπευτικούς διαύλους απειλών, όπως η μη εξουσιοδοτημένη πρόσβαση, οι επιθέσεις μέσω side-channel, η διαρροή προσωπικών δεδομένων, η παραποίηση firmware και ο συμβατότητα συσκευών. Επιπλέον, αξιολογεί κριτικά τους υφιστάμενους μηχανισμούς και μεθόδους ασφαλείας που έχουν σχεδιαστεί για τον μετριασμό αυτών των κινδύνων, συμπεριλαμβανομένων των πρωτοκόλλων ελαφριάς κρυπτογράφησης, των πολυπαραγοντικών μεθόδων ελέγχου ταυτότητας (MFA), των συστημάτων ανίχνευσης εισβολών (IDS) και των τεχνικών ανίχνευσης ανωμαλιών, με στόχο την ενίσχυση της ανθεκτικότητας έναντι εξελιγμένων απειλών.

Πέρα από τις τεχνικές διαστάσεις, η παρούσα διατριβή τονίζει τον κρίσιμο ρόλο της ευαισθητοποίησης και εκπαίδευσης των χρηστών για τη διατήρηση ασφαλών περιβαλλόντων έξυπνου σπιτιού. Παρά τις τεχνολογικές βελτιώσεις στα κατασκευαστικά πρότυπα και τις συνθήκες διαβίωσης, η υποκειμενική αίσθηση ασφάλειας συχνά παραμένει ανεπαρκής, οδηγώντας σε εντατικοποίηση της έρευνας για προηγμένες τεχνολογίες προστασίας. Η αυξημένη ανασφάλεια, ιδιαίτερα στα πυκνοκατοικημένα αστικά κέντρα, έχει οδηγήσει στην αξιοποίηση τεχνικών Τεχνητής Νοημοσύνης (AI) και Μηχανικής Μάθησης (ML) για τον σχεδιασμό ευφυών

συστημάτων πρόληψης και απόκρισης σε απειλές, ενισχύοντας την αίσθηση φυσικής και ψηφιακής ασφάλειας.

Σε αυτό το πλαίσιο, έχουν αναπτυχθεί εφαρμογές που βασίζονται σε τεχνικές Βαθιάς Μάθησης (Deep Learning – DL), οι οποίες μετασχηματίζουν την παραδοσιακή κατοικία σε αυτοματοποιημένο, προσαρμοστικό και ασφαλές σύστημα. Η διατριβή εστιάζει στη διπλή συμβολή του DL: την ενίσχυση της κυβερνοασφάλειας και την διεπιστημονική εφαρμογή της σε πεδία όπως η ιατρική, όπου παρατηρούνται εξαιρετικά αποτελέσματα. Ιδιαίτερη έμφαση δίνεται στην αναλυτική παρουσίαση του αλγορίθμου backpropagation τόσο σε γραμμικά όσο και σε μη γραμμικά τεχνητά νευρωνικά δίκτυα, καθώς και στη μελέτη του προβλήματος XOR ως κλασικού παραδείγματος μη γραμμικότητας.

Η Μηχανική Μάθηση επιδεικνύει υψηλή αποτελεσματικότητα στην ανάλυση ανθρώπινης δραστηριότητας, με κορυφαία εφαρμογή στην αναγνώριση προσώπου, η οποία αποτελεί θεμελιώδη παράμετρο για την εξατομίκευση της διαχείρισης και της ασφάλειας σε περιβάλλοντα έξυπνου σπιτιού. Η ανάγκη για επεξεργασία μεγάλου όγκου δεδομένων σε πραγματικό χρόνο, σε συνδυασμό με αυξημένες απαιτήσεις υπολογιστικής ισχύος, καθιστούν αναγκαία τη χρήση των υπολογιστικών υποδομών ομίχλης (fog) και υπολογιστικού νέφους (cloud computing), οι οποίες αξιοποιούνται για αποδοτική επεξεργασία εικόνας, αναγνώριση προσώπων και διάκριση ανθρώπινων σιλουετών.

Τα προαναφερθέντα υποσυστήματα συγκροτούν ένα ολοκληρωμένο πλαίσιο ασφάλειας βασισμένο σε αρχιτεκτονικές DL και εκπαιδευμένα μοντέλα ML. Με βάση τα ευρήματα της παρούσας μελέτης, τεκμηριώνεται ότι η εφαρμογή αυτών των τεχνολογιών προωθεί σημαντικά την επίτευξη πλήρους ασφάλειας στην οικία, ανταποκρινόμενη σε ένα επείγον κοινωνικό αίτημα, ειδικά υπό το πρίσμα της αυξανόμενης εγκληματικότητας.

Τέλος, η διατριβή προτείνει μελλοντικές κατευθύνσεις έρευνας για την περαιτέρω ενίσχυση της ασφάλειας στα έξυπνα σπίτια μέσω IoT. Οι προτάσεις περιλαμβάνουν την ανάπτυξη ενοποιημένων και ισχυρών προτύπων ασφαλείας, βελτιωμένων μεθόδων ελέγχου ταυτότητας συσκευών, καθώς και την αξιοποίηση ευφυών μηχανισμών ανίχνευσης εισβολών που βασίζονται σε τεχνικές ανάλυσης ανωμαλιών

και συνεχή μάθηση. Η αντιμετώπιση αυτών των τεχνικών προκλήσεων είναι καθοριστική για την πραγματοποίηση του οράματος των πλήρως λειτουργικών, ασφαλών και ανθεκτικών σε απειλές έξυπνων σπιτιών με δυνατότητες IoT, που διασφαλίζουν την ιδιωτικότητα και την ψηφιακή κυριαρχία των χρηστών.

Λέξεις-κλειδιά: έξυπνο σπίτι, μηχανική μάθηση, βαθιά μάθηση, ανατροφοδότηση, νευρωνικά δίκτυα, αναγνώριση προσώπου, σιλουέτας και δραστηριοτήτων, ασφάλεια, ιδιωτικότητα, ανθεκτικότητα.

Table of Contents

Acknowledgments xi
Abstract xiii
Περίληψη xvi
List of Figures and Tables xxi
Acronyms xxii
CHAPTER 1 1
Introduction 1
1.1 Related Work 5
CHAPTER 2 8
Machine Learning 8
2.1 The Deep Learning Method in Machine Learning 8
2.2 Deep Learning Contribution in Medicine 11
2.3 Deep Learning with Backpropagation Algorithm to Neural Networks 18
2.4 The Training Method for Linear Neurons 22
2.5 The Training Method for Non-Linear Neurons 23
2.6 X-OR Problem Simulation 26
CHAPTER 3 30
3.1 Machine Learning Human Activities in Smart Home 30
3.2 Face Recognition System in Smart Home 32
3.3 Methods of Facial Recognition 33
3.4 Face Recognition Application Using Fog and Cloud Computing Technologies 35
3.5 Human Silhouette/Figure Recognition System 36
CHAPTER 4 38
Smart-Home Ecosystem 38
4.1 IoT in Smart Homes 38
4.2 Infotainment Devices 43
4.3 Physical Home Security and Monitoring 43
4.4 Ambient Living Devices 49
4.5 Other Aspects and Actuators 51
CHAPTER 5 54
5.1 Architectural Structure of IoT Ecosystems 54

5.2 Threats Faced by a Smart Home and Related Countermeasures 57
5.3 Best-Practices Guide for a Secure Smart Home 66
5.4 Directions for Future Research 70
CHAPTER 6 73
Bibliography 75

List of Figures and Tables

Figure 1 *Basic building blocks of IoT ecosystems.*.....2

Figure 2. *A Network with Multiple Levels.*.....19

Figure 3 *Output value calculation.*.....20

Figure 4. *Pattern Recognition.*.....21

Figure 5. *A network for the X-OR problem.*.....27

Figure 6. *Summary of network learning.*.....29

Figure 7. *Face Alignment Module.*.....35

Figure 8. *Generate a 3D-aligned face image from a 2D face image. The steps from (A–H).*.....36

Figure 9. *Smart-home threats and countermeasures*.....58

Table 1. *Number of Cycles, Solving the X-OR problem*.....28

Table 2. *Latency and Bandwidth Comparison.*.....53

Table 3. *Fog VM Migration Performance.*.....53

Table 4. *Summary of threats and examples of countermeasures per IoT layer*.....71

Acronyms

WSN (wireless sensor networks)

AI (artificial intelligence)

IoT (Internet Of Things)

DDoS (Distributed Denial of Service)

IDS (Intrusion-Detection System)

SDN (Software-Defined Network)

RPL (Routing Protocol for Low-Power)

6LowPan (Low-PowerWireless Personal Area Networks)

QoS (Quality of Service)

RFID (Radio Frequency Identification)

WSN (Wireless Sensor Network)

NN (Neural Networks)

RNN (Recurrent Neural Network)

DN (Deep networks)

NLP (Natural Language Processing)

ML (Machine Learning)

ANN (Artificial Neural Network)

FDA (Diagnostic Data Program)

CAD (Computer Aided Diagnosis)

EHR (Electronic Health Records)

DL (Deep Learning)

abbreviated TND (train artificial neural networks)

HAR (Human Activity Recognition)

RFID (Radio-Frequency Identification)

AVSS (Advanced Video and Signal Surveillance)

VM (Virtual Machine)

SVM (Support Vector Machine)

LAN (Local Area Network)

DoS (Denial of Service)

ASR (Automatic Speech Recognition)

NLU (Natural Language Understanding)

TEE (Trusted Execution Environment)

AR (Augmented Reality)

VR (Virtual Reality)

AES (Advanced Encryption Standard)

GPS (Global Positioning System)

IEC (International Electrotechnical Commission)

IIC (Industrial Internet Consortium)

IIRA (Industrial Internet Reference Architecture)

OCF (Open Connectivity Foundation)

NIST (National Institute of Standards and Technology)

API (Application Programming Interface)

ECC (Curve Cryptography)

PRNU (Photo Response Non-Uniformity)

OEM (Original Equipment Manufacturer)

PKI (Public Key Infrastructure)

ISP (Internet Service Provider)

CPS (Cyber–Physical System)

QKD (Quantum Key Distribution)

SVM (Support Vector Machine)

CHAPTER 1

Introduction

The use of wireless technologies in Smart Homes is examined by highlighting both the benefits and drawbacks associated with the diverse range of heterogeneous devices found in household appliances. These variations create challenges in effectively monitoring both the home environment and its occupants. Key issues include the deployment of wireless devices that operate without interference, capable of detecting user behaviors within monitored areas, as well as the observation of elderly individuals—who serve as typical case studies. In these scenarios, the user's self-assessment of their activities can enhance the overall effectiveness of the provided services. [1]. Wireless architectures have been integrated as adaptable and unobtrusive tools, exemplifying a fully autonomous environment. By leveraging existing advanced solutions that form the foundation of modern architectures, there is an opportunity to simplify the system and lower costs. This is achieved by exploiting the unique properties of wireless signals to monitor presence, track locations, and identify residents' movement and behavior patterns.

Wireless technologies commonly utilized in smart homes and wireless sensor networks (WSNs) have been validated as the most effective architectural solution for implementing movement detection services. Key smart home functionalities include distributed smart energy metering and elderly care support, both of which drive the adoption of wireless systems in domestic settings. This trend is reinforced by the increasing average age of the global population and the ongoing energy crisis. The benefits primarily stem from employing cost-efficient wireless networks designed to monitor and analyze user behavior, particularly for elderly individuals [2].

Specialized methods have been researched and assessed for detecting daily activities, and have been incorporated into advanced wireless architectures aimed at monitoring and tracking user behavior. Non-invasive wireless approaches have been implemented, utilizing electromagnetic detection alongside commonly available mobile devices like smartphones. Numerous electromagnetic technologies exist that contribute to maintaining the simplicity of smart home systems while ensuring user acceptance. Notably, the ELEDIA Research Center at the Department of Computer Engineering and Computer Science (DISI), University of Trento, Italy, has

documented practical applications of wireless technologies that have become integral to everyday life [3].

In recent decades, computer science has seen remarkable progress, particularly regarding the use and accessibility of the Internet [4,5]. Today, nearly all contemporary activities rely on Internet-based services [6,7]. More recently, Internet of Things (IoT) technologies have quickly become an integral part of daily life [8,9]. This technology enables the development of fully automated environments, or at minimum, ongoing efforts to establish such systems. This is achieved through the use of the Internet alongside smart devices like smartphones, home assistants, smart TVs, wearable devices, smart locks, thermostats, robotic vacuums, and others. Figure 1 illustrates the core components of an IoT ecosystem.

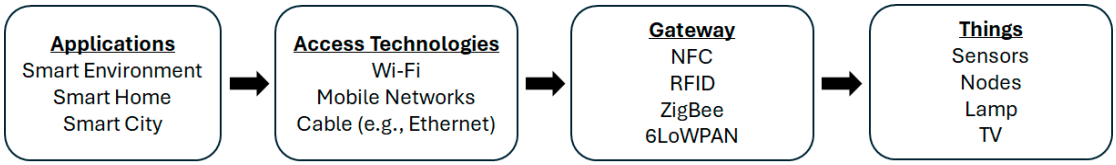


Figure 1. *Basic building blocks of IoT ecosystems.*

These intelligent devices employ similar sensors to gather data and work collaboratively to create an automated environment that delivers a variety of services to contemporary society. Such services enhance convenience, efficiency, and security, especially within smart home settings. Research by Cisco [10] highlights the rapid increase in personal Internet-enabled devices: from 12 billion connected devices in 2010 to 25 billion in 2015, 50 billion in 2020, and an estimated 1 trillion by 2035. The IoT leverages this expanding network of interconnected devices to provide diverse services through a single interface, often the user's smartphone. Nonetheless, managing and securing smart homes via IoT presents considerable challenges because of the heterogeneous and independent nature of the devices involved. While many smart home devices offer standalone functionalities, their need to interact and cooperate is hindered by the variety of technologies and communication protocols they use. The diversity of technologies in smart home devices introduces vulnerabilities that expose these systems to potential attacks, compromising overall security. The ISO-27005 security framework [11] highlights that weaknesses within interconnected device environments can lead to complete security breaches, enabling malicious actors to infiltrate networks and remotely access personal data and management functions. For instance, in 2014, footage from 73,000 Internet-connected cameras was leaked online, and by 2016, Internet-connected devices faced

cyberattacks on average every two minutes [12]. Research by HP [13] revealed that about 70% of smart devices are susceptible to security threats, with 90% of personal data collected during device setup being intercepted during testing phases. In today's rapidly evolving digital era, technology is deeply embedded in our daily lives. Modern cyber-physical systems are driving innovative applications that once seemed futuristic. Smart homes and intelligent environments, which are the central focus of this thesis, exemplify this trend. Advanced automation, artificial intelligence, assisted living, security, robotics, and personalized healthcare are among the prominent use cases. Increasingly, people are adopting these technologies in their residences and other smart settings such as hotels, workplaces, and factories.

Humans have become integral components of this cyber ecosystem. As system users, they serve as the primary "subjects" within these typically personalized environments. Consequently, safeguarding residents from both cyber-related risks and possible physical dangers is critically important.

Nonetheless, the foundational technologies and their interactions within such intricate systems complicate their protection. Components like IoT, cloud computing, diverse smart devices and sensors, electronic and mobile commerce, social media, and AI contribute to this complexity. Their rapid development in recent years has outpaced regulatory frameworks and the responsible, informed use of technology. Governmental and standardization initiatives tend to advance slowly, often taking years to yield outcomes—by which time the technology has already evolved further. User awareness about inherent risks remains limited; adoption practices are still immature; and the private sector lacks sufficient numbers of skilled professionals, such as technicians and engineers, to provide adequate support. Consequently, multiple challenges persist in securing smart-home environments, including the following.User awareness level: Users are always considered one of the weak links on the cyber risk chain, and usually, home users are not aware of the cyber threats related to smart-home devices, or may not know how to properly secure them. This can lead to weak passwords, false configurations, failure to update software, and other security vulnerabilities.

- Complexity: Smart homes can be complex systems with many devices, sensors, and services. This complexity can make it difficult to manage security and identify vulnerabilities.

- Interoperability and Heterogeneity: Smart-home devices are often developed by different manufacturers and use different communication protocols, which makes it difficult to ensure that they can all work together securely.
- Remote access: Smart-home devices often allow for remote access via Internet connection, which increases the risk of unauthorized access by attackers. This is especially concerning as many users may not secure their remote access properly.
- Limited resources: Smart-home devices often operate with limited resources, such as low power consumption, limited memory, and processing power. This makes it challenging to implement strong security protocols.
- Lack of regulation: There are currently no standardized security regulations for smart home devices, which means that security measures can vary widely between different devices and manufacturers.

This thesis undertakes a comprehensive analysis of security challenges within home environments and proposes corresponding mitigation strategies [14, 15, 16, 17]. Given the pervasive reliance on Internet connectivity, users bear a substantial responsibility to become informed about the safe and proper use of their smart devices, as well as the potential risks and threats involved [18, 19, 20, 21]. Contemporary IoT frameworks conceptualize the technology as comprising four distinct layers—application, perception, network, and physical—each vulnerable to specific attack vectors [22]. This study systematically investigates threats according to these layers and offers targeted recommendations for their mitigation. Furthermore, unlike prior research, this work also explores the unique security considerations associated with prominent categories of smart devices, including home assistants, smart TVs, AR/VR systems, smart locks, and environmental sensors.

Also addresses several key aspects, including an introduction to cybersecurity within contemporary smart-home IoT environments and a review of relevant surveys. It examines the modern smart-home ecosystem alongside the diverse array of IoT devices it encompasses. The study analyzes the architectural framework of IoT settings and provides a comprehensive review of potential attacks, corresponding countermeasures, and the challenges inherent in securing smart homes. Furthermore, it discusses the findings derived from this research and proposes security guidelines aimed at protecting the various components and system layers within smart-home environments. Finally, the thesis highlights promising directions for future research and concludes with reflections on ongoing and prospective work in this domain.

1.1 Related Work

Research efforts have contributed to the development of essential guidelines aimed at enhancing system security and safeguarding personal data [17, 23, 24]. These studies have identified critical vulnerabilities within the IoT architecture, particularly emphasizing the heterogeneity of smart devices and their Internet connectivity, which collectively increase the risk of unauthorized access to home environments [25, 26, 27]. A primary focus of this body of work is the prevention of emerging threats and the formulation of effective countermeasures against potential system attacks. Yang and Sun [28] provide a comprehensive analysis of the security challenges confronting smart-home systems. Their research explores the architectural components of smart homes, delineates six inherent and contextual characteristics, and frames the ongoing conflict between "spears" (cyber-attack techniques) and "shields" (defensive strategies). Additionally, the thesis examines various security frameworks and evaluation methods, while also considering the convergence of smart-home technologies with other domains such as blockchain, cloud computing, and artificial intelligence.

The authors recommend that future research efforts should prioritize the development of unified architectures, address inherent resource constraints, mitigate fragmentation issues, and strengthen the security of code and firmware in smart-home systems. The survey underscores the necessity of emphasizing security concerns in smart-home research, rather than focusing predominantly on commercialization, to ensure the creation of robust and dependable solutions. Dahmen et al. [29] offer an extensive review of smart-home technologies and their contributions to enhancing resident security. Their work examines a variety of smart-home functionalities aimed at detecting, identifying, and responding to potential security threats. The authors provide a comparative analysis between commercial products and academic research, highlighting sensing mechanisms designed to identify anomalies or breaches, evaluate threat severity, and implement automated response systems to effectively manage these risks. Bastos et al. [30] provide an in-depth investigation of the proliferation and security implications of IoT devices within domestic settings. Their study discusses how the increasing ubiquity of these devices expands the IoT ecosystem while simultaneously exacerbating security vulnerabilities. They emphasize the surge in IoT deployments alongside the anticipated growth in security-related expenditures needed to mitigate associated risks. The thesis reviews key IoT components, such as sensors,

actuators, and network protocols, which both facilitate connectivity and elevate the potential for security breaches. Prominent challenges include vulnerability to Distributed Denial of Service (DDoS) attacks and weak authentication mechanisms that enable unauthorized access. The authors advocate for the integration of robust security measures throughout the IoT development lifecycle, as well as continual system updates to counteract evolving cyber threats, thus aiming for secure IoT adoption in everyday life and infrastructure.

Particular research focus is placed on intrusion-detection systems (IDSs) for smart homes [31, 32], which are critical for maintaining system security. Furthermore, network quality of service (QoS) remains a significant concern. Although Software-Defined Networks (SDNs) provide scalable solutions, they may simultaneously introduce new vulnerabilities. Researchers are thus challenged to devise strategies that safeguard security protocols such as the Routing Protocol for Low-Power and Lossy Networks (RPL) and IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), while preserving secure networking and high QoS [33, 34, 35]. IDS implementations must deliver effective performance with minimal energy consumption and processing latency, and also enable rapid response to threats. Despite these demanding requirements, the considerable benefits that IoT systems offer for home security motivate continued efforts to overcome the limitations faced by IDS technologies [26, 27, 28, 29, 30, 31].

Radio Frequency Identification (RFID) technology plays a significant role in enhancing the security of intrusion detection systems (IDS) by enabling effective interfacing among smart devices within a smart home environment [36]. This study will explore the various security challenges and solutions pertinent to smart homes, beginning with a detailed examination of the architectural layers within IoT systems. A primary vulnerability of IoT ecosystems lies in the heterogeneity of smart-home devices, which poses substantial security risks [27, 37, 38].

A proposed approach to securing smart home environments involves the deployment of Wireless Sensor Networks (WSNs) integrated with IoT technologies to deliver a range of services [39, 40, 41]. The sensors within these networks monitor and track movement, while collaborating to provide valuable data to the system. Current research focuses on enhancing the privacy and security of the entire home ecosystem, addressing various threats and attacks that IoT-enabled smart homes may encounter. Solutions are typically classified according to the specific threats faced by the system. Nevertheless, ensuring the privacy and confidentiality of data remains a

critical challenge. The rapid proliferation of intelligent devices, especially mobile technologies, is outpacing the evolution of security protocols and systems, resulting in widespread use of IoT devices that often lack adequate protection measures [42].

Ensuring the security and privacy of smart-home environments necessitates the development of smart devices fortified with robust security protocols as a primary priority. Within such environments, smart devices autonomously communicate and exchange data, which is then aggregated and processed by a centralized unit. The system must be capable of identifying potentially malicious devices attempting unauthorized access by masquerading as legitimate components. A major challenge stems from the heterogeneity of interface standards among smart devices, underscoring the need for a unified architecture supported by strong protection mechanisms. Consequently, ongoing research focuses on enhancing security, integrity, confidentiality, and energy-efficient methodologies [30,43]. Given that most IoT devices are characterized by low power consumption and limited memory capacity, the system must operate with minimal computational overhead and energy use. However, reliance on cloud or fog computing layers for data transmission introduces vulnerabilities to data interception, while physical disruptions such as natural disasters pose risks of system failure. Additionally, variations in security protocols and device capabilities challenge system interoperability and resilience. The system's exposure to diverse attack vectors, categorized by the IoT architectural layers, will be explored in subsequent sections.

Several surveys focus not on the smart-home environment as a whole, but rather on specific categories of devices. For instance, Xu et al. [44] investigated the security aspects of home assistants, Santani et al. [45] explored vulnerabilities in smart TVs, and Guzman et al. [46] studied mixed-reality technologies. This thesis adopts contemporary design frameworks (e.g., [22]) that segment the smart-home system analysis into four layers—application, perception, network, and physical—and advocate for a unified architectural model. Beyond providing a general overview of IoT characteristics and their security ramifications, this research delves into the security specifics of a variety of devices commonly found in residential settings. These include smart-home assistants, televisions, AR/VR headsets, robotic vacuums, electronic locks, sensors, and more. To the best of our knowledge, this work constitutes the first comprehensive study to systematically examine the security challenges associated with such an extensive range of smart-home devices, while aligning with contemporary smart home and IoT architectural paradigms.

CHAPTER 2

Machine Learning

2.1 The Deep Learning Method in Machine Learning

Machine learning emerged as a subset of artificial intelligence (AI) aimed at enabling machines to learn from data input and processing. AI, as an academic discipline, focuses on how machines acquire knowledge and make decisions based on data. Early research in AI explored various approaches, with particular emphasis on neural networks (NN) methodologies. The development of machine learning gained significant momentum after 1992, revolutionizing problem-solving techniques, whereas prior to that, traditional AI methods predominated. Specifically, machine learning employs statistical and probabilistic techniques, contrasting with the symbolic approaches characteristic of classical AI. Traditional machine learning algorithms tend to have relatively simple structures, such as decision trees. In these conventional approaches, engineers must supply the system with extensive domain knowledge through large datasets and often manually adjust algorithms to ensure that the machine produces the desired outputs.

In contrast, deep learning employs backpropagation, enabling the system to learn autonomously by iteratively correcting errors through feedback mechanisms. During this process, input data and neuron weights are continuously adjusted until the desired output is achieved. Deep learning relies on executing complex algorithms within multilayered neural networks, allowing the machine to emulate the human brain's capacity for acquiring new knowledge [46]. In recent years, debate has persisted among researchers regarding the relationship between machine learning and artificial intelligence; while many view machine learning as a subset of AI, a substantial number argue that they constitute distinct fields [47]. Importantly, deep learning (DL) enables computer models composed of multiple processing layers to generate hierarchical data representations. This approach has notably advanced domains such as speech recognition, visual object recognition, and object detection, as well as facilitated significant progress in areas like drug discovery. DL leverages the backpropagation algorithm to iteratively adjust internal parameters, for instance within a camera system, to refine feature representations at each neural network layer. These advancements have led to substantial breakthroughs in image, video, speech, and audio processing. Applications incorporating machine learning techniques are

expanding rapidly across diverse societal sectors, including web search engines, social media content filtering, the semantic web, and e-commerce. Furthermore, such methodologies have become increasingly prevalent in consumer electronics like cameras and smartphones. Machine learning systems are widely employed for tasks such as object detection in images, speech-to-text conversion, and personalized content matching—thereby enhancing the relevance of search results based on individual user interests. Increasingly, these applications harness a combination of techniques derived from deep learning frameworks.

Traditional machine learning techniques initially had limited capabilities for processing complex data. Over many years, efforts have been made to develop pattern recognition systems or machine learning methods capable of effectively deriving meaningful outputs from unstructured input data—such as pixel values in images—by constructing suitable internal feature representations or groupings. These representations enable the learning system to detect or classify patterns upon data input, often utilizing classifiers. Thus, machine learning encompasses a variety of methods that assist intelligent systems in discovering the necessary representations for detecting or classifying human movements. Deep learning, a prominent subset of machine learning, employs multiple layers of representation (hidden layers in a neural network), where each layer receives input from the previous one, starting from raw data at the first level. The final output is produced through the synthesis of several iterative transformations, yielding classified and identified data. During these classification processes, higher-level representations emphasize input features that are most relevant for accurate separation and categorization, while filtering out irrelevant and redundant variations to improve efficiency. For example, an image is initially represented as a series of pixel values at the first layer, where simple features such as edges at specific orientations and locations are detected. The second layer identifies patterns by recognizing arrangements of these edges, invariant to small positional changes. Subsequent layers integrate these patterns into larger shapes corresponding to known objects, and further layers ultimately recognize complete objects as combinations of these shapes.

The primary distinction between deep learning and classical machine learning lies in the learning process: deep learning divides the learning task into multiple stages, with each stage focusing on extracting specific features. The combined learning across these hierarchical levels results in improved performance. In contrast, classical machine learning relies on a general-purpose learning process applied

uniformly without layered feature extraction. Due to its staged approach, deep learning is particularly well-suited to solving problems that have historically posed significant challenges in the field of artificial intelligence. For instance, it can uncover complex, high-dimensional structures by revealing one dimension at each stage of processing. Deep learning has been successfully applied in areas such as image recognition, speech recognition, brain circuit reconstruction, and predicting the effects of DNA mutations on genetic expression related to diseases. Moreover, it shows promising potential in other domains, including natural language understanding, emotion analysis, and real-time language translation [48].

Unsupervised learning—conducted in environments not strictly controlled—has played a pivotal role in the renewed interest in deep learning, surpassing the earlier success of purely supervised learning methods. The foundational principle of unsupervised learning aligns with the way humans and animals learn: predominantly through observation rather than explicit instruction. Human understanding of the world often emerges from observing patterns and relationships, a process more adaptable than simply labeling objects. For instance, human vision is an active and dynamic process, receiving sequential stimuli from optic neurons through a focused and selective high-resolution function. Deep learning has also made remarkable advances in natural language understanding, a domain with significant current impact and substantial room for future development. Systems utilizing Recurrent Neural Networks (RNNs) are now capable of comprehending sentences or entire documents by learning strategies that process sequential data inputs [49].

Deep networks (DNs) have been successfully applied to unsupervised learning in individual modalities such as text, images, or audio. More advanced architectures now enable learning across multiple modalities simultaneously—e.g., processing real-time video and audio—supporting a broad range of cooperative tasks [50]. With deep learning, machines increasingly mimic the way the human brain learns, shifting from explicit programming to autonomous learning based on experiential data. Much like humans, these systems continuously improve by observing data, receiving feedback, and iteratively classifying and recombining known concepts to learn more complex ones. This hierarchical prioritization of concepts across multiple levels underpins the learning process. Deep learning is now integral to numerous applications, including facial recognition, search engines, targeted advertising, content retrieval, and interactive environments such as video games [51].

2.2 Deep Learning Contribution in Medicine

The advancement of deep learning within the broader scope of machine learning—and consequently the progress of artificial intelligence (AI)—is increasingly producing positive societal outcomes, including the creation of millions of new jobs and notable contributions to economic growth. This emerging growth trajectory is largely driven by "smart decision-making mechanisms" implemented through intelligent systems. Among the most transformative applications of AI is its integration into the medical field, where it has yielded highly encouraging results and is regarded as a promising avenue for future innovation.

AI technologies are already embedded in everyday life, often without users fully realizing their presence. Examples include voice-activated virtual assistants such as Apple's Siri, Amazon's Alexa, and translation tools like Google Translate—all of which leverage Natural Language Processing (NLP) techniques. Significant financial investment underscores the importance of AI, with up to 30 billion dollars invested in AI research over the past five years. Notably, 90% of research and development efforts in the field are led by major technology companies such as Google and Microsoft.

The widespread adoption of AI across scientific disciplines—particularly in medicine—has sparked heightened interest among medical technology providers. To enhance the market appeal of their products, many companies now emphasize the use of AI methodologies in their development processes [52].

Artificial intelligence (AI) is increasingly gaining popularity and acceptance in the field of medicine, owing to its ability to manage, analyze, and visualize highly complex and voluminous medical data. This area of application is projected to experience significant growth in the coming years. Patient care involves the coordination of multiple interdependent and variable stages, each of which may influence or be influenced by others. Intelligent systems can navigate this complexity by continuously learning from data through iterative training and experience. By optimizing the algorithms they employ, such systems are capable of deriving meaningful insights that support clinical decision-making and improve patient outcomes.

Nevertheless, despite the early and optimistic predictions emerging from the field of computer science, it has taken considerable time for AI to reach its current level of maturity and practical applicability within healthcare.

Let begin with Machine Learning (ML), which is widely regarded as a subfield of Artificial Intelligence (AI). Much like humans learn through continuous exposure to stimuli and data from their environment, machines also learn and improve their performance by processing increasing volumes of data over time. ML is a promising field with broad applicability in optimizing processes and enabling intelligent resource allocation mechanisms.

The basic functioning of ML can be illustrated through a simple example involving the classification of Iris flower species. Initially, developers identify the key features that distinguish different types of Iris—such as the shape and size of petals and sepals, color distribution, and specific morphological traits. These features are compiled into a structured dataset, often referred to as the "training dataset," which contains labeled examples of various Iris species.

Once this dataset, composed of hundreds of high-quality, annotated images, is fed into the learning algorithm, the model is trained to associate specific feature combinations with corresponding species. Remarkably, after adequate training, the machine acquires the ability to identify a previously unseen Iris species based on its learned knowledge. This capacity to generalize beyond the training data is a central strength of ML systems.

The performance of ML models improves significantly with the richness and diversity of the training dataset. Moreover, learning is driven by feedback mechanisms such as backpropagation, which allow the model to refine its internal parameters iteratively. In effect, the machine dynamically reconfigures itself based on its errors and experiences—continuously evolving without direct human intervention.

IBM Watson for Health is perhaps one of the most representative and well-known applications of machine learning in the medical domain [53]. It serves as a powerful decision-support tool for healthcare professionals, offering access to vast repositories of structured and unstructured medical data and delivering insights in real time with minimal processing delays. Regardless of the physician’s geographic location, Watson can access global medical knowledge, analyze clinical evidence, and provide validated recommendations, contributing to safer and more effective decision-making. This paradigm is often referred to as cognitive computing, emphasizing the system’s ability to simulate human reasoning while continuously learning from new data.

It is important to note that the effectiveness of a machine learning system—whether in healthcare or in simpler use cases such as flower recognition—depends

heavily on the engineer's ability to accurately define the relevant features and data parameters. In the Iris classification example, for instance, the quality and precision of the input features (e.g., petal length, color patterns) directly influence the performance and reliability of the model. This critical dependency highlights the importance of expert domain knowledge in both the design and training phases of machine learning systems.

The task of the programmer in machine learning is to convert data into a format that is comprehensible to the machine—commonly referred to as machine-readable data. This process typically involves transforming information into structured datasets, such as relational tables where attributes and values are explicitly defined. However, in the healthcare domain, this is particularly challenging since most medical data are unstructured, comprising clinical notes, free-text observations, and graphical records rather than neatly organized numerical fields.

Given the inherent complexity of data preprocessing, software engineers responsible for developing machine learning models must demonstrate a high level of expertise. They are tasked with selecting or engineering features—that is, deriving meaningful input variables from raw data—that will ultimately enhance the model's performance. In practice, however, the utility of a given feature is often unknown until the model is trained and tested. This leads to iterative development cycles where engineers repeatedly adjust features, retrain models, and evaluate performance until the desired level of accuracy is achieved. While this process is inherently time-consuming, the continuous addition of new and diverse training datasets enables the gradual improvement of predictive accuracy.

The challenge of processing vague, voluminous, and unstructured data has led researchers to emulate biological systems, especially the human brain. This pursuit gave rise to Artificial Neural Networks (ANNs), which are inspired by the structure and functioning of biological neurons. ANNs are composed of interconnected layers of nodes (or artificial neurons), mimicking the complex, branched connectivity of neurons in the brain. Each node processes input data and passes information to subsequent layers, creating a multi-layered logical framework that enables the extraction of patterns and relationships from raw input. Through this biologically inspired architecture, machines are now capable of organizing and interpreting complex datasets with increasing autonomy and sophistication.

Each level in a deep learning architecture presents its own challenges in interpreting the data received from the preceding level. Although the foundational

concept of multi-layered neural networks has existed for decades, it was not until the early 2000s—thanks to advances in hardware, particularly the development of high-performance GPUs (e.g., by NVIDIA)—that deep learning became computationally feasible. These advancements enabled the training of neural networks with dozens, or even hundreds, of layers, giving rise to the term deep learning. Such architectures are capable of handling highly complex and voluminous data, facilitating a high degree of automation in pattern recognition and decision-making.

Artificial Neural Networks (ANNs) can now process input data and autonomously generate outputs without the need for explicit human-defined features. For example, given a sufficiently large dataset of Iris flower images, deep learning algorithms can independently learn to identify the distinguishing characteristics of each species, without prior knowledge or manual feature engineering. Similarly, they can distinguish among human faces without the use of pre-defined traits. In contrast to traditional machine learning approaches—where algorithms rely on structured data and manually selected features such as "mouth," "eyes," or "nose"—deep learning models can infer such features automatically. Notably, systems like Google's deep facial recognition algorithms can identify the same person (e.g., “Uncle Bob”) across multiple images, even when certain features (e.g., hair color or facial shape) were never explicitly specified.

This capability marks a significant departure from earlier AI techniques. For instance, Google's DeepMind has developed a system based on Deep Q-Learning that can learn to play the arcade game Breakout without any prior knowledge of the game mechanics or visual components. The model does not need to be told what a ball or paddle is; rather, it learns to interpret and respond to environmental stimuli through repeated interaction and feedback. This approach—reminiscent of how children learn from experience—allows the machine to autonomously develop strategies and behaviors to achieve desired outcomes, underscoring the powerful potential of deep reinforcement learning in artificial intelligence.

During gameplay, an AI system employing deep reinforcement learning—such as Deep Q-Learning—can autonomously discover the objective of hitting the ball with the paddle in order to succeed. Through continuous interaction, trial-and-error, and feedback, the AI incrementally improves its performance, ultimately becoming a highly skilled and competitive player. Remarkably, the knowledge and strategies acquired in one domain (e.g., a particular video game) can be adapted and transferred to other, similar tasks, demonstrating the flexibility and generalization

capabilities of deep learning systems. This is a significant contrast to human learning: for instance, a lawyer is unlikely to possess the skills required to practice medicine or plumbing without extensive retraining.

In the medical field, deep learning has led to the development of groundbreaking applications. One such application involves the U.S. Food and Drug Administration (FDA), which supports the use of AI to model and predict drug interactions. These models can estimate drug toxicity levels with high precision, potentially eliminating the need for the decade-long process of animal testing, thereby addressing serious ethical concerns.

Another critical application of deep learning in healthcare is in cancer detection through medical imaging. Machine learning models trained on large datasets of X-rays have achieved diagnostic accuracy levels comparable to, or in some cases exceeding, those of experienced radiologists. By recognizing patterns associated with various types of cancer, these systems offer significant potential in early diagnosis and treatment planning.

Moreover, the integration of historical patient data into AI-driven analytics systems enables hospitals and clinics to enhance decision-making processes. These systems can be used to optimize resource allocation, improve clinical workflows, and streamline patient care, ultimately contributing to more efficient and effective healthcare delivery [54].

The term Computer-Aided Diagnosis (CAD) is relatively modern, having been introduced approximately fifty years ago. Initially applied in pulmonary imaging—including chest radiographs and computed tomography (CT)—CAD refers to the use of computational systems to assist in or automate diagnostic decisions. In the context of lung imaging, CAD systems have demonstrated improved diagnostic accuracy compared to traditional rule-based methods, especially when operating under controlled conditions. This field continues to evolve rapidly, and recent advancements in deep learning have significantly enhanced its capabilities and performance.

Historically, CAD was first introduced in scientific literature in 1966, highlighting the potential role of computers in aiding repetitive radiological tasks. The early conceptualization of CAD proposed a general framework: converting optical radiographic images into numerical sequences (what we now describe as feature vectors), which could be processed by a computer to facilitate diagnosis. This early idea paved the way for the development of classifier-based systems that analyze image-derived vectors during testing to predict or classify medical conditions.

In recent years, the convergence of a massive influx of digital health data, advancements in computational capabilities, and the development of sophisticated machine learning algorithms has dramatically accelerated progress in CAD. The emergence of deep learning, in particular, has proven transformative. Deep learning models, especially convolutional neural networks (CNNs), are capable of learning high-level semantic features directly from raw input data, bypassing the need for manual feature engineering. These models exhibit superior performance in image-based diagnostics, including the detection of pulmonary nodules, pneumonia, and other thoracic abnormalities.

Furthermore, improvements in computational infrastructure—such as the use of powerful GPUs, reduced energy consumption, and high-speed data storage—have enabled the training and deployment of complex deep learning models at scale. This has expanded the use of CAD systems from academic and research environments to real-world clinical settings, providing predictive accuracy and interpretability that can significantly assist radiologists and other medical professionals in making informed decisions [55].

Deep Learning (DL) has emerged as the leading method in terms of performance across a wide range of machine learning techniques, particularly in the domain of pattern recognition. In healthcare, DL has enabled the development of advanced solutions based on large and complex datasets, facilitating the automatic extraction of relevant features and significantly reducing the need for human intervention. This constitutes a major advantage in the medical domain, where unstructured data—especially from medical imaging—present a formidable challenge. The ability of deep learning to process and learn from such unstructured sources has contributed to the evolution of a new interdisciplinary field: Medical Informatics and Bioinformatics.

In addition to unstructured data, a substantial amount of medical information is encoded in structured formats, such as Electronic Health Records (EHRs), which provide comprehensive insights into a patient’s medical history, diagnoses, treatments, and pathology. When combined with imaging data, such as cytological analyses used to detect and classify tumors, DL systems can analyze various complex attributes, including tumor stage, spread, and morphological features. This integration supports a more holistic understanding of a patient's condition, enabling more accurate and personalized medical decision-making.

The incorporation of deep learning and broader artificial intelligence (AI) techniques into clinical workflows holds the potential to significantly enhance diagnostic accuracy, support evidence-based treatment planning, and ultimately improve patient outcomes. Furthermore, the adoption of such technologies may increase the operational reliability and diagnostic consistency of healthcare facilities. Despite these advancements, several technical challenges persist—such as the need for explainability, data privacy, standardization, and robust model generalization—highlighting areas where further research and development are still critically required.

Clinical patient data is often costly to obtain, while data from healthy individuals tends to constitute a large proportion of the overall health datasets. Deep learning algorithms generally perform best on balanced datasets, and a common approach to address class imbalance is to augment the data by generating synthetic or combined samples. However, this practice raises concerns about the reliability and validity of artificially fabricated clinical data, which may affect model performance and generalizability. Another critical limitation of deep learning is its heavy reliance on large volumes of high-quality training data. The scarcity of clinical data—due to both its cost and strict privacy regulations related to medical confidentiality—poses significant, and sometimes insurmountable, barriers to the deployment of machine learning models in healthcare.

Despite these challenges, deep learning continues to drive the development of robust, continuous, and effective medical monitoring and diagnostic tools. These advancements are expected to play a pivotal role in shaping the future landscape of medical research and clinical practice.

It is worth noting that the rise of deep learning has been strongly supported by major IT corporations such as Google, Facebook, and Baidu, which hold numerous patents in this domain and possess vast data repositories and advanced computational infrastructure. Many researchers have increasingly applied deep learning to data mining techniques, aiming to extract meaningful patterns related to health diagnostics by leveraging freely available clinical datasets to advance their work. From a positive perspective, this has cultivated heightened expectations for the capabilities of machine learning in healthcare. However, it is important to avoid the misconception that deep learning represents a “silver bullet” capable of solving every medical challenge. In conclusion, deep learning has revitalized neural network research and emerged as a crucial and powerful tool in modern medicine—one that, when properly applied, has the potential to drive revolutionary advances in healthcare [56].

2.3 Deep Learning with Backpropagation Algorithm to Neural Networks

The backpropagation algorithm is a class of methods used to effectively train artificial neural networks (ANNs), employing an optimization technique based on gradient descent that utilizes the chain rule of calculus. A key feature of backpropagation is that the network is continuously fed with updated input data to iteratively adjust the weights (or loads) of the neurons. This process is repeated until the weights converge to values that enable the network to produce the desired output, thereby achieving the intended behavior through training.

When designing the network, the outputs of neurons after applying the activation function must be considered. Unlike static systems, these outputs are automatically fed forward as inputs to subsequent layers, allowing the network to modify its behavior dynamically based on the results produced. During training, this feedback is used to compute the gradients of the loss function with respect to the neuron weights. The backpropagation algorithm calculates these gradients, while stochastic gradient descent (SGD) employs them to iteratively update the weights and optimize the system's performance [57].

The primary objective of a neural network trained through supervised learning is to identify a function that, given appropriate inputs, will generate the desired outputs. The backpropagation method achieves this by performing multiple automatic feedback cycles to set the weights in such a way that the network can correctly interpret new input data and produce accurate outputs.

A typical neural network architecture consists of an input layer, one or more hidden (internal) layers, and an output layer. The input layer is composed of neurons that primarily serve to receive input signals without performing significant processing. The hidden layers contain neurons that process the input signals received from the previous layer and forward the results to the next layer. Finally, the output layer consists of neurons that receive signals from the hidden layers and provide the final output of the network without further processing.

There is no fixed rule governing the number of hidden layers or the number of neurons within each layer; these parameters vary depending on the specific problem. As illustrated in Figure 2, neurons from different layers are connected by weighted links. The connectivity pattern between neurons is flexible: in some cases, each

neuron may be connected to every neuron in subsequent layers, resulting in a fully connected network with the maximum number of connections.

Alternatively, a network with multiple levels of each neuron could be connected to just one other neuron (the minimum number of connections it can have). In intermediate cases there are usually some connections between neurons. Obviously, the number of onnections, especially for full wiring is very large. If we have N neurons, then the number of connections in complete wiring is N (N - 1)/2. The training process is similar to the sensor, but has some essential differences. The signal comes to each input level neuron (the first level). Multiply by the corresponding weight w of each conclusion. In each neuron the arriving products are added and the S is calculated, as in the sensor model. However, there is an essential difference here. While in the sensor the sum is compared to θ, here something different happens. There is a representation (activation) function, which is typical of the network, and which is used each time to calculate what the output value will be [58]. Suppose the output value is o. A commonly used function is shown on Figure 3.

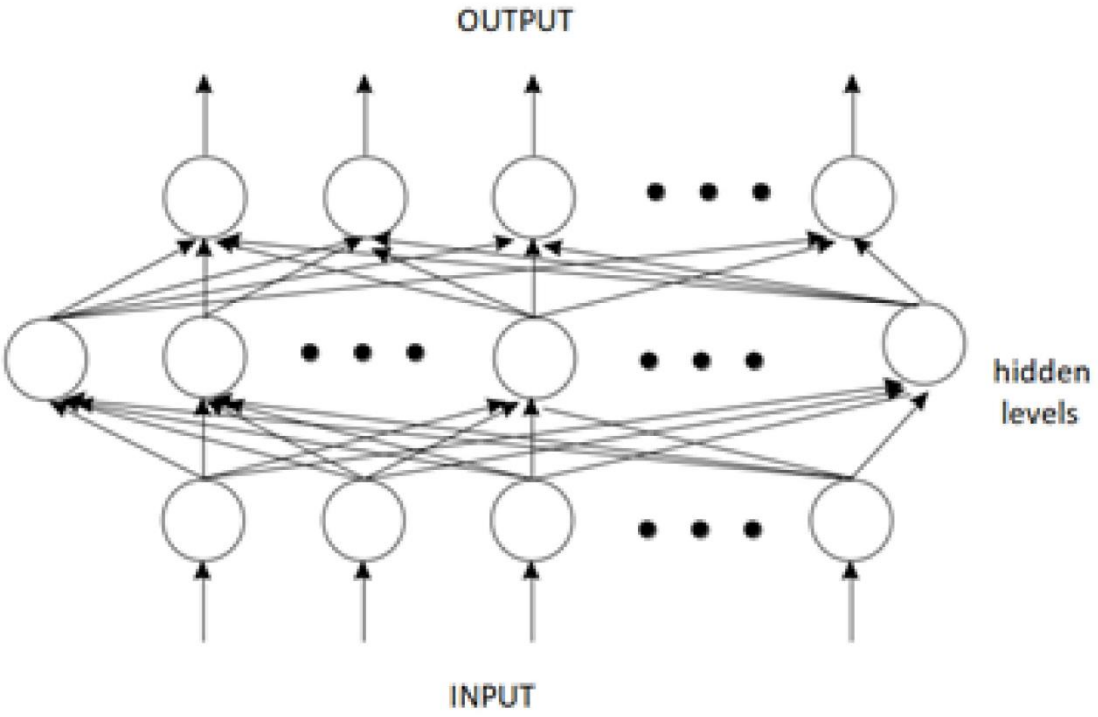


Figure 2. *A Network with Multiple Levels.*

The value of o is always $0 < o < 1$, for any value of input S. This is important, because that way we are sure that there will be no cases where the output takes large values or tends to infinity. This curve is called sigmoid because of its shape. It is an ideal function, because it behaves well for all price sizes. For small values of S the

slope is large, and so the output is not almost 0. Accordingly, for large values of S the slope is normal, so that the network cannot be saturated. Another property of this function is that its derivativealso behaves well, which is necessary in the training process, below. We easily show the following equation:

$$\frac{-\partial o}{\partial S} = o(1-o) \qquad (1)$$

Another name for the function o is compressed function, because it compresses any value of S in the interval between 0 and 1. We also observe that this function is non-linear, a necessary condition for the network to be able to generate signal representation. This overall process is a cycle, i.e., a passage, entry-exit-entry, and summarizing includes the following steps:

- We get a pattern from the many. We enter it at the entry level.
- We calculate the output.
- We promote it in the same way at all levels up to the final output level.
- We calculate the error.
- We change weights, returning from exit to entry, one by one, and level-by-level.
- We move on to the next template.

$$o = \frac{1}{1+e^{-S}}$$

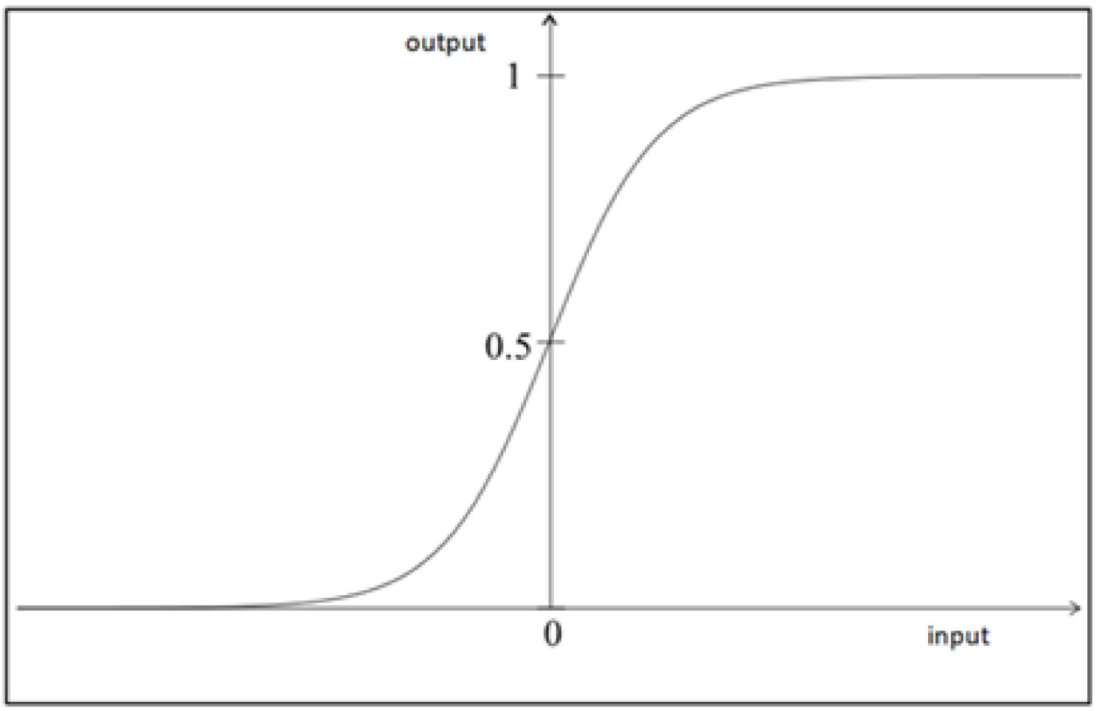


Figure 3. *Output value calculation.*

At the end of a cycle, repeat the process for as many cycles as needed, until the error is small enough. The tolerance for the error is given in advance, and standard values are a few % units, e.g., 2 or 5%. An example of a target pattern pair is given in Figure-4, where the letter A is plotted on a grid. If any line passes through a square, then the input to the corresponding neuron is 1. Otherwise, the input is 0. The output can be a number representing A, or another set of 0 and 1 [58]. For the whole alphabet we need 24 network training pairs, one pair for each letter. The error reversal training method uses the same general principles as the Delta rule. The system first takes the inputs of the first standard and with the procedure described previously produces the output. It compares the output value with the target value. If there is no difference between the two nothing happens and we move on to the next pattern. If there is a difference then we change the values in such a way that this difference is reduced [59].

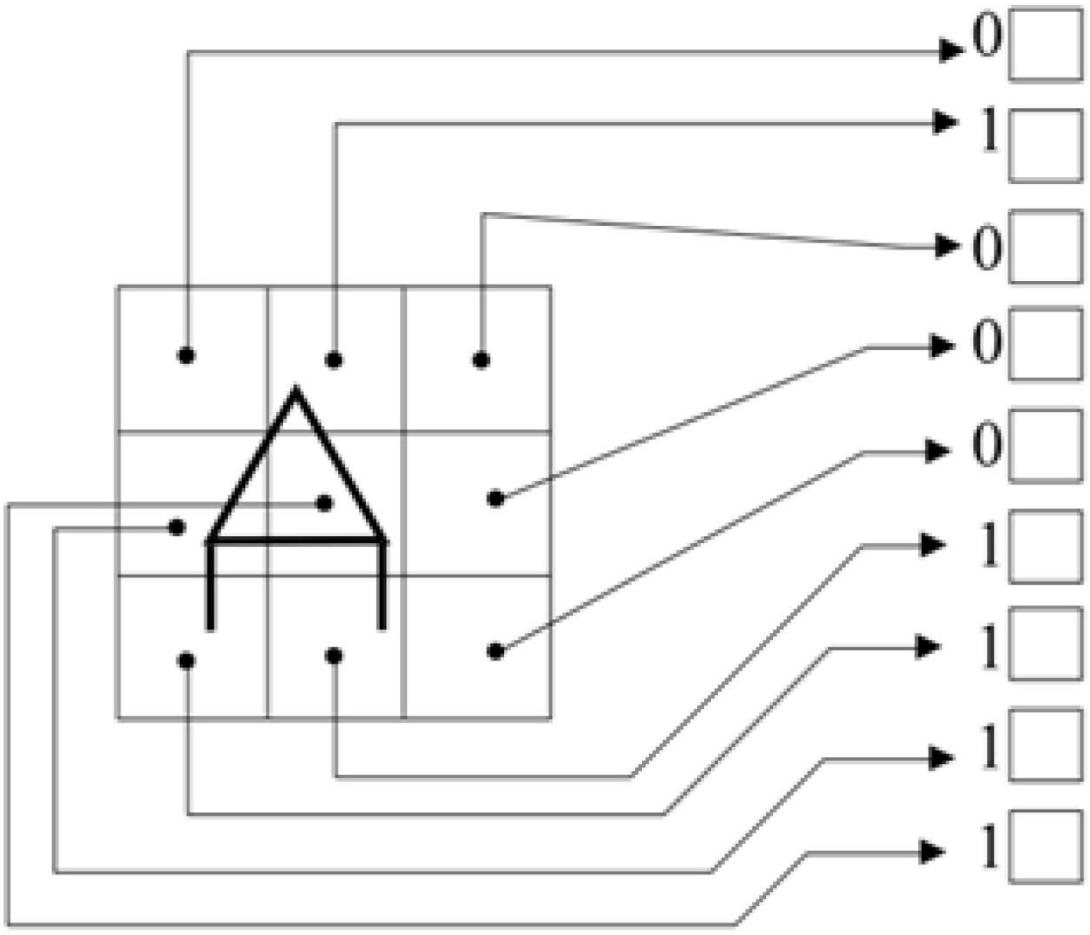


Figure 4. *Pattern Recognition.*

2.4 The Training Method for Linear Neurons

In this methodology, the objective for each neuron and for each input pattern is to minimize the squared difference between the neuron's actual output and the desired target value. This means that the derivative of the error with respect to each weight *w* determines how the weight should be adjusted. Specifically, the change in the weight is proportional to this derivative, following the Delta rule, and is scaled by a negative learning rate constant. This process corresponds to performing gradient descent on the error surface in the weight space, where the height of the surface represents the error magnitude. By moving weights in the direction of the steepest descent, the network iteratively reduces the error until convergence.

The above applies to linear units of neurons.

$$E_P = \frac{1}{2}\sum_j (t_{pj} - o_{pj})^2 \qquad (2)$$

where Ep is the error (input-output difference) in template p, tpj and opj is the target and output of neuron j for template p. The total error E is:

$$E = \sum_p E_p \qquad (3)$$

For linear units we apply the Delta rule, and we actually have a gradient descent in E. We show that:

$$\frac{-\partial E_p}{\partial w_{ji}} = \delta_{pj} x_{pi} \qquad (4)$$

When there are no hidden units then the derivative is calculated immediately. We use the chain rule and write the derivative as a product of two other derivatives: one derivative of the error with respect to the output of the neuron on one derivative of the output with respect to weight.

$$\frac{\partial E_p}{\partial w_{ji}} = \frac{\partial E_p}{\partial o_{pj}} \frac{\partial o_{pj}}{\partial w_{ji}} \qquad (5)$$

The first derivative tells us how the error in the output of the j neuron changes, while the second part tells us how much the change in wji changes this output. This is how we directly calculate the derivatives. The contribution of neuron j to the error is proportional to *d*pj, since we have linear units.

$$o_{pj} = \sum_i w_{ji} x_{pi} \tag{6}$$

from which we conclude that:

$$\frac{\partial o_{pj}}{\partial w_{ji}} = x_{pi} \tag{7}$$

Substituting Equation (5) we see that:

$$-\frac{\partial E}{\partial w_{ji}} = \sum_p \frac{\partial E_p}{\partial w_{ji}} \tag{8}$$

exactly as we want. Combining the latter equation with the observation that:

$$\frac{\partial E}{\partial w_{ji}} = \sum_p \frac{\partial E_p}{\partial w_{ji}} \tag{9a}$$

leads us to the conclusion that the change in wji after a complete cycle, where we present all the patterns, is proportional to this derivative, and therefore the Delta rule applies a sloping descent to E. Normally w should not change during the cycle where we present the various patterns, one by one, but only at the end of the cycle. However, if the training rate is low, no big mistake is made and the Delta rule works properly. Finally, we will find the values of w that minimize the error function [59, 60].

2.5 The Training Method for Non-Linear Neurons

We have shown that the Delta rule results in gradient descent on the squared error sum for networks with linear activation functions. In the case where there are no hidden layers, the error surface forms a convex, bowl-shaped function with a single global minimum. Consequently, gradient descent will always converge to the optimal weights *w*.

However, when hidden layers are introduced, calculating derivatives becomes less straightforward, and the error surface is no longer convex. This means there may be multiple local minima where the training process can get stuck. Despite this, as we will show, there is an effective method to compute these derivatives, and in practice, the problem of local minima rarely hinders the overall training of the network.

The networks considered here have a multi-layer, feedforward structure, where signals propagate in one direction—from the input layer at the bottom, through

the hidden layers, and finally to the output layer at the top. Each neuron in every layer processes its input independently. The neuron applies a nonlinear activation function to the weighted sum of its inputs, producing an output that becomes the input to the neurons in the next higher layer. For such a nonlinear function the output is:

$$S_{pj} = \sum_i w_{ji} o_{pi} \qquad (9b)$$

where opi is the input signal of neuron i. Therefore,

$$o_{pi} = f_j(S_{pj}) \qquad (10)$$

where f is a differentiable and increasing function. Linear functions are not enough here, because their derivative is infinite at the threshold, and zero at other values. We suppose that:

$$\Delta_p w_{ji} \approx -\frac{\partial E_p}{\partial w_{ji}} \qquad (11)$$

where E is the error function (sum of squares). Here we put this derivative as a product of two derivatives: one that gives the change in error with respect to the change in the input value, and one that gives the change in the input value with respect to the change in weight. So:

$$\frac{\partial E_p}{\partial w_{ji}} = \frac{\partial E_p}{\partial S_{pj}} \frac{\partial S_{pJ}}{\partial w_{ji}} \qquad (12)$$

We see that:

$$\frac{\partial S}{\partial w_{ji}} = \frac{\partial}{\partial w_{ji}} \sum_k w_{jk}\, o_{pk} = o_{pi} \qquad (13)$$

We define that:

$$\delta_{pj} = -\frac{\partial E_p}{\partial S_{pj}} \qquad (14)$$

where *d*pj = (opj -tpj), as well as opj = Spj when the neurons are linear. So we have:

$$-\frac{\partial E_p}{\partial S_{pj}} = \delta_{pj} o_{pi} \qquad (15)$$

This indicates that to apply the sloping c to E we must make the changes to w

as follows:

$$\Delta_p w_{ji} = \eta \delta_{pj} o_{pi} \qquad (16)$$

just like in the usual Delta rule. Now we need to calculate the correct δpj for each neuron in the network. Here, we put this derivative as a product of two derivatives: one that gives the error change as a function of the output, and one that gives the output change as a function of the input change. So, we have:

$$\delta_{pj} = -\frac{\partial E_p}{\partial S_{pj}} \frac{\partial o_{pj}}{\partial S_{pj}} \qquad (17)$$

but we have:

$$\frac{\partial o_{pj}}{\partial S_{pj}} = f'_j(S_{pj}) \qquad (18)$$

which is the derivative of the activation function for neuron j, calculated at the input signal Spj to this neuron. Now we compute the first derivative in the equation δpj. Here you need attention. We calculate this factor differently if the neuron is at the output level or internally. In case it is at the output level then:

$$\frac{\partial E_p}{\partial o_{pj}} = -(t_{pj} - o_{pj}) \qquad (19)$$

which is the same result as with the usual Delta rule. By substituting the two factors we get:

$$\delta_{pj} = (t_{pj} - o_{pj}) f'_j(S_{pj}) \qquad (20)$$

for neurons that are at the output level. For neurons that are internal there is the problem that we have no tpj, i.e., we do not have target values. In this case we have:

$$\sum_k \frac{\partial E_p}{\partial (S_{pk})} \frac{\partial (S_{pk})}{\partial o_{pj}} = \sum_k \frac{\partial E_p}{\partial (S_{pk})} \frac{\partial}{\partial o_{pj}} \sum w_{ki} o_{pi}$$
$$= \sum_k \frac{\partial E_p}{\partial (S_{pk})} w_{kj} = -\sum_k \delta_{pk} w_{kj} \qquad (21)$$

Substituting similarly we get:

$$\delta_{pj} = f'_j(S_{pj}) \sum_k \delta_{pk} w_{kj} \qquad (22)$$

These equations give the way in which all d, for all neurons in the network, are calculated, and which are used to calculate the change in w across the network. This procedure is considered to be a general delta rule. In summary, the above procedure can be summarized in three equations. First, we apply the general Delta rule in the same way as the general rule. The w in each level changes by a quantity that is proportional to the error signal δ, and also proportional to the output o. That is,

$$\Delta_p w_{ji} = \eta \delta_{pj} o_{pi} \qquad (23)$$

The other two equations give the error signal. The process of calculating this signal is

a cyclic process that starts at the output level. For a neuron at the output level the error is:

$$\delta_{pj} = (t_{pj} - o_{pj}) f'_j(S_{pj}) \qquad (24)$$

where f'j (Spj) is the derivative of the activation function. For neurons in hidden levels is given by:

$$\delta_{pj} = f'_j(S_{pj}) \sum_k \delta_{pk} w_{kj} \qquad (25)$$

These three equations form a circle. The system repeats as many cycles as it takes to train [59].

2.6 X-OR Problem Simulation

As i showed, at my work Vardakis G. et. al. "Smart home: Deep learning as a method for machine learning in recognition of face, silhouette and human activity in the service of a safe home" [59], the solution of a well-known X-OR problem with a grid containing a hidden layer, as described above and shown in Figure 5. The network structure includes two neurons at the input level, one neuron at the hidden level and one at the output level.

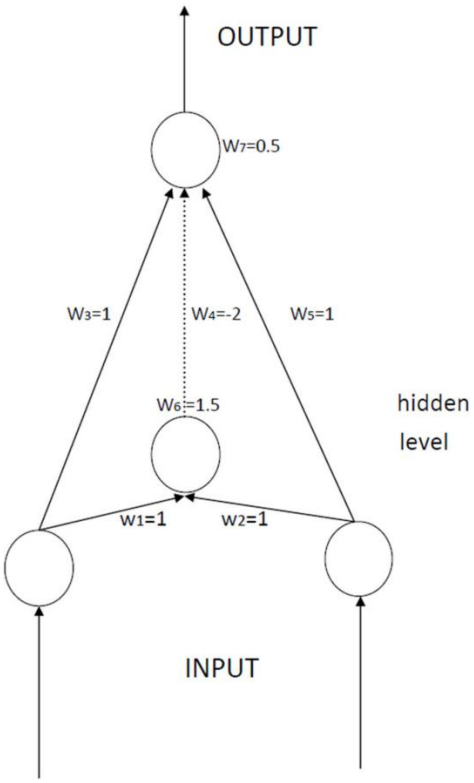


Figure 5. *A network for the X-OR problem.*

The connections are as in the figure 5. It is necessary that the entrances go both to the hidden level and to the exit directly. This problem is of didactic importance, as its solution includes all the details of the backward propagation technique, and for this reason we will outline its solution by a simulation method, following one by one the steps and equations [62]. We use an equation to calculate the outputs of each neuron, the sigmoid function, as:

$$o_{pj} = \frac{1}{1 + e - (\sum_i w_{ji} o_{pi} + \theta_j)} \qquad (26)$$

where θj is the predisposition parameter (or predisposition) and which in a way plays the role of the threshold. The values of predisposition, θj, will be taught in the network, as well as the values of the other weights w. Indicates the weight w of a unit (neuron) that is always active. The derivative opj (1 - opj) has a maximum for opj = 0.5, and approaches its minimum when opj approaches 0 or 1, such that $0 \leq$ Opj ≤ 1. The change in a w is proportional to its derivative, and so the ws will change more if we have a mean value, i.e., neither active nor inactive. This feature gives the system solution stability. It should also be noted that when checking for output values 0 or 1, it is impossible to get exactly these values unless we have w that tends to infinity. Usually, it is enough when we get 0.1 and 0.9, even if we mention 0 and 1. This

accuracy is reached. The equation of the change of w has a constant, the n, which represents the training rate of the network. The larger the n, the greater the changes in w, and the faster the network trains. However, if it does not become very large, then this leads to oscillations, and so we are forced to not be able to increase it much. One way to increase the pace of training and avoid fluctuations is to include another term that indicates the momentum of the system. Thus, the equation becomes:

$$\Delta w_{ji}(n+1) = \eta \delta_{pj} o_{pi} + \alpha \Delta w_{ji}(n) \qquad (27)$$

where n denotes the cycle, or the rate of training, and *a* is the constant that takes into account the previous changes of w when calculating the new change. This is a form of system momentum that essentially filters out high-frequency changes to the error surface. Usually, we get a value of *a* which is *a* = 0.9. We first assume that the weights w1 = w2 = w3 = w5 = 1. The value w4 = -2 from the hidden neuron to the output neuron renders the output neuron inactive when both inputs are active at the same time. The numbers inside the neurons are the values of i. At the hidden level θ = 1.5 because then this neuron will only fire when both neurons of the first level are active. The value θ = 0.5 on the output neuron makes this neuron active only when it receives a positive signal greater than 0.5. On the output neuron side, the hidden level neuron appears as another input unit. It sees it as if there were three input values [15,16,17]. Of course, these prices are purely indicative, and not necessary for the solution of the problem. Applying the simulation method now, we solve the X-OR problem, so that the network can successfully find the patterns and the number of cycles needed to do this, given in Table 1. In the solution given below we start with random values of w that range in the range -0.3 < x < 0.3.

η	α	Number of Cycles
0.1	0	82,000 ± 24,000
0.9	0	8000 ± 2200
0.1	0.1	8100 ± 2200
0.9	0.9	870 ± 230

Table 1. *Number of Cycles, Solving the X-OR problem.*

The values in table are averages of ten embodiments, with different values of w each time. We observe that the standard deviation has a large value, which shows that the solution is directly dependent on the initial w. Summarizing the solution of this problem, we give the flow chart, as well as the equations in Figure 6 below.

calculation of δ

δ[4]=der(o[4])•(t-o[4])

δ[3]=der(o[3])•(d[4]•w[4])

δ[2]=der(o[2])•(δ[4]•w[5]+δ[3]•w[1])

δ[4]=der(o[1])•(δ[4]•w[3]+δ[3]•w[1])

where : der(o[1]) the derivative of the corresponding output

calculation of Δw	change of w
Δw[1]=η•δ[3]•o[1]	wi[n+1]= wi[n]+Δwi[n]+p. Δwi[n-1]
Δw[2]=η•δ[3]•o[2]	όπου i=1…..7
Δw[3]=η•δ[4]•o[1]	
Δw[4]=η•δ[3]•o[3]	
Δw[5]=η•δ[4]•o[2]	
Δw[6]=δ[3]	
Δw[7]= δ[4]	

Figure 6. *Summary of network learning [15,16,17].*

CHAPTER 3

Machine Learning-Human Recognition

3.1 Machine Learning Human Activities in Smart Home

A smart home today, empowered by deep learning, offers advanced services in both safety and healthcare by recording and recognizing faces and human activities using depth cameras. Current efforts focus on optimizing such systems to enhance daily life quality, especially for the elderly, through continuous and daily monitoring of human activities.

Inside the home, the system continuously records and gradually acquires knowledge and experience in recognizing behaviors and events. This valuable knowledge improves system performance, thereby raising the quality of services provided. The system supports real-time life logging by recognizing human activities based on depth imaging. A depth imaging device captures depth silhouettes during human activity recordings, extracting critical information from these silhouettes—specifically from body parts essential for identifying activities. The system learns to recognize human actions by training on these depth images.

Initially, the system is trained using a depth camera to detect and record human movement, then to recognize the presence of human activity, identify human silhouettes, extract distinguishing features, and classify different activities. Ultimately, this process enables the machine to maintain a continuous record of human life and activities, allowing it to recognize daily human behaviors in real time through camera input.

A modern approach evaluated against traditional life recording systems running on conventional PCs demonstrated that applying Radon transformations on depth silhouette features significantly improves recognition accuracy. Real-time experiments confirmed the system's feasibility and functionality, showing that it can effectively generate lifetime logs of human activities in smart homes.

Such technology contributes to safer and more convenient living environments by integrating sensor technologies—such as motion sensors, video cameras, and RFID—with systems that store records of users' daily activities. The system includes a "life diary," a virtual log containing comprehensive information about an

individual's daily actions collected via various sensors and video recordings. This diary can be incorporated into everyday smart devices, providing applications ranging from healthcare services for the elderly to security monitoring in smart homes.

A life recording system refers to a mechanism that continuously creates files documenting the indoor daily activities of residents (e.g., in smart homes or offices) by recognizing human activity (Human Activity Recognition—HAR). Typically, multiple sensors such as motion detectors, video cameras, and RFID are employed in HAR systems. These systems enable ongoing monitoring and documentation of inhabitants' daily routines, making HAR one of the fundamental processes in smart living environments.

Based on these automatically recorded Human Activity Recognition (HAR) life systems, it is possible to analyze human life patterns to improve quality of life by examining daily habits and routine actions—such as sleeping, medication intake, office schedules, or meal times—tailored to an individual's lifestyle. Life recording systems typically utilize electronic devices, including portable motion sensors and video cameras. The motion sensors, worn or carried by the user, capture motion signals that are recorded and analyzed to extract features characteristic of different human activities. These features enable the system to recognize activities and thereby construct a detailed routine of the user's daily life.

Portable motion sensor technologies have been widely studied and presented for daily activity recognition, including at the 2014 11th IEEE International Conference on Advanced Video and Signal Surveillance (AVSS), where both conventional and novel life recording approaches were compared. When compared to traditional systems relying on depth silhouettes, life recording systems employing Radon transform-based recognition demonstrated improved accuracy for nearly all smart home activities.

Experimental results showed that the proposed life recording system with Radon-based recognition achieved an activity recognition rate as high as 89.33%, outperforming conventional systems, which scored 71.25% and 78.58% using depth silhouettes. This technology is highly applicable across many daily life domains, particularly for consumers in smart homes, where it offers significant benefits for elderly residents by providing continuous health monitoring. The system effectively creates an activity diary for elderly individuals, aiming to enhance their quality of life through improved safety and personalized care [64, 65, 66, 67].

3.2 Face Recognition System in Smart Home

A facial recognition system automatically identifies or verifies a person from a digital image or video. One common method involves comparing selected facial features from the image with those stored in a real-time database. Today, face recognition systems are nearly real-time and accessible in many affordable consumer applications. These systems respond uniquely to each user, providing personalized services tailored to the specific home environment and individual user data. As such, face recognition technology has become a powerful tool for enhancing quality of life in smart homes.

In a smart home, the system operates over a home network that continuously monitors and records the environment using low-cost equipment [68, 69, 70, 71, 72, 73]. To manage computational load efficiently, face recognition processing is divided into stages: (1) gradual "pruning" for face detection, (2) coarse-to-fine face extraction for smoothing and normalization, and (3) face recognition using sequential discriminant analysis. Implementations in experimental home networks have demonstrated recognition rates exceeding 95% with processing speeds of 3 to 4 frames per second, making this a fast and reliable built-in solution for smart home applications.

Unlike traditional systems that require controlled environments and offer limited recognition capabilities, this system is designed for real-world conditions without operational restrictions, achieving high accuracy and robustness. Its main advantages include processing efficiency and low cost, while covering all fundamental functions: face detection, feature extraction and normalization, and final face recognition. Incremental improvements at each step enhance the system's robustness and efficiency.

The face recognition system performs well using inexpensive hardware, making it ideal for everyday consumer use where user-friendly interfaces and affordability are paramount. Although face recognition typically demands powerful processors, this system employs distributed processing—detecting faces at the entrance, extracting features, and conducting recognition on a multimedia server within the home—to optimize performance.

Currently, the HomeFace system effectively recognizes frontal faces with off-plane rotations up to ±20 degrees; future research is needed to handle larger head rotations [74].

3.3 Methods of Facial Recognition

Using deep machine learning with neural networks, a system can recognize, classify, and align facial images. Starting from a 2D image, the machine is capable of producing an aligned 3D representation of the face. The process begins with classification and alignment of the 2D face image, which forms the basis of face recognition. Unique characteristics of a person are encoded as a set of feature vectors, which provide a unique identity for the individual depicted.

The algorithm identifies a person's identity from images or video without human intervention. Face recognition in everyday, unconstrained images—captured under real-world conditions—is a groundbreaking and transformative concept. Despite attempts to mimic human brain and eye functions, current systems still exhibit significant error rates. Most advances have been made with 2D face images taken in controlled and limited environments, relying on methodologies such as sketching, control systems, and intelligent biometric identification. However, system capabilities degrade significantly in uncontrolled, real-world conditions involving variations in lighting, facial expressions, aging, and pose [68, 69].

Face recognition applications typically integrate systems, methods, non-transient computer-readable media, and neural networks for face image alignment, sorting, and verification. For identity verification, a second image may be used to confirm whether both images belong to the same individual. In some implementations, a 3D face model is extracted from an aligned 2D image. While recognition occurs primarily in the 2D domain, classification is performed using the aligned 3D representation.

In practical applications, a set of 2D keypoints is identified on the face image. These keypoints serve as "anchor" points that enable the construction of the corresponding 3D shape and the aligned 3D face image. During deep learning-based processing, these keypoints can be represented as triangles or anchors, which may be mapped on either the front or back of the 3D model. The aligned 3D face is generated by applying an affine transformation to each triangle defined by these anchor points.

Further, additional keypoint sets can be detected within the 2D image, enabling reconstruction of the full 2D face. The deep neural network (DNN) architecture typically includes a max-pooling layer and a convergent layer, which extract the aligned 3D facial points through connections to adjacent layers. Each

connected layer is configured to capture correlations between these 3D aligned points, representing them as feature vectors.

These feature vectors serve as descriptors for the 3D image and are normalized to a predefined range. With learned filters, each pixel in the 2D image is associated with a 3D aligned point. The machine autonomously learns to optimize these filters based on the training data vectors it processes.

Face recognition systems compare the processed 2D face image against a face database, where images are grouped into sets, each corresponding to a specific person [70, 71]. Each set of features corresponds to a unique face ID. During classification, the DNN assigns unique values to each face ID by processing between adjacent layers. Based on this classification, the system separates and identifies faces by matching feature vectors to known identities, as illustrated in Figures 7 and 8.

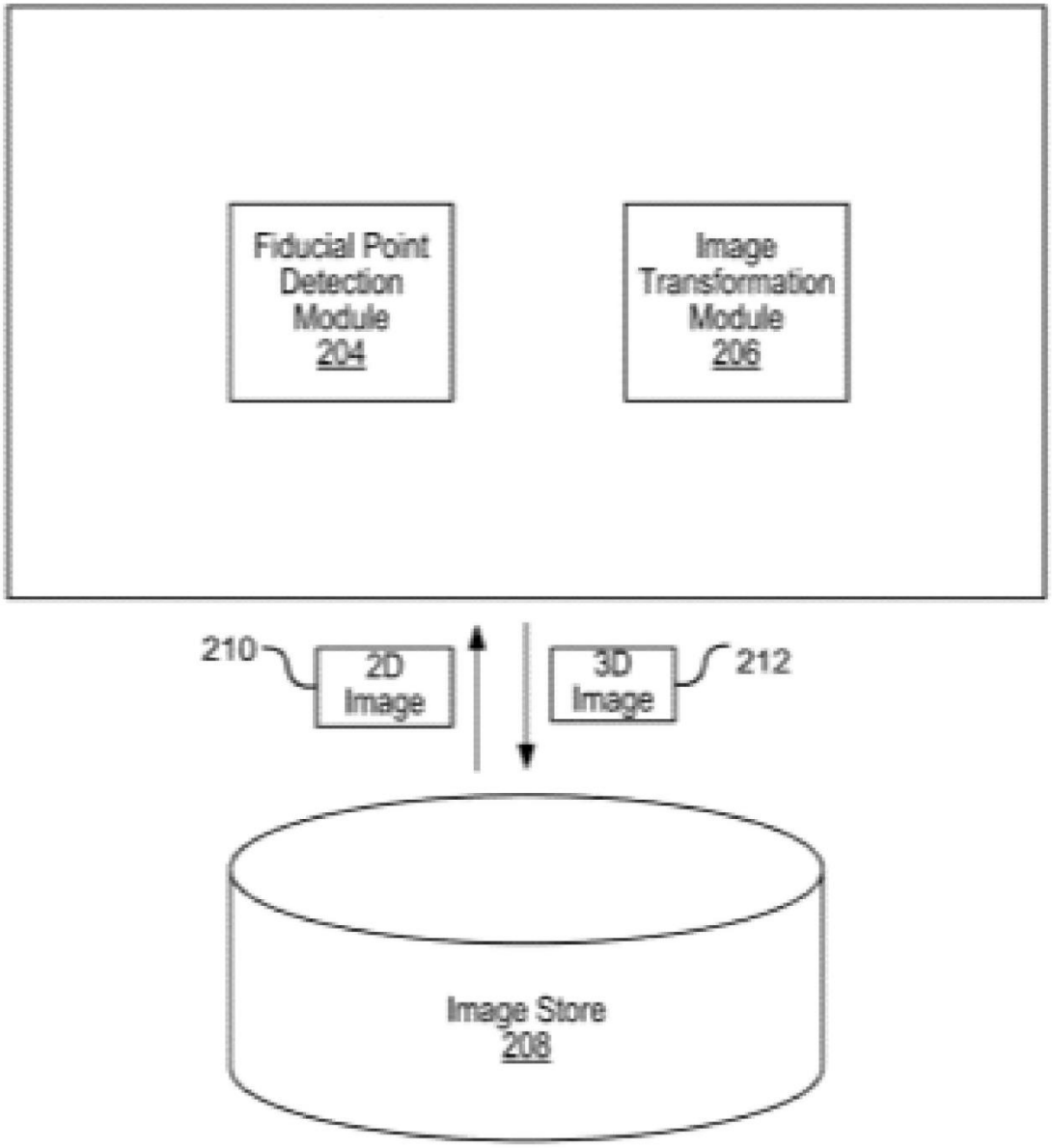


Figure 7. *Face Alignment Module.*

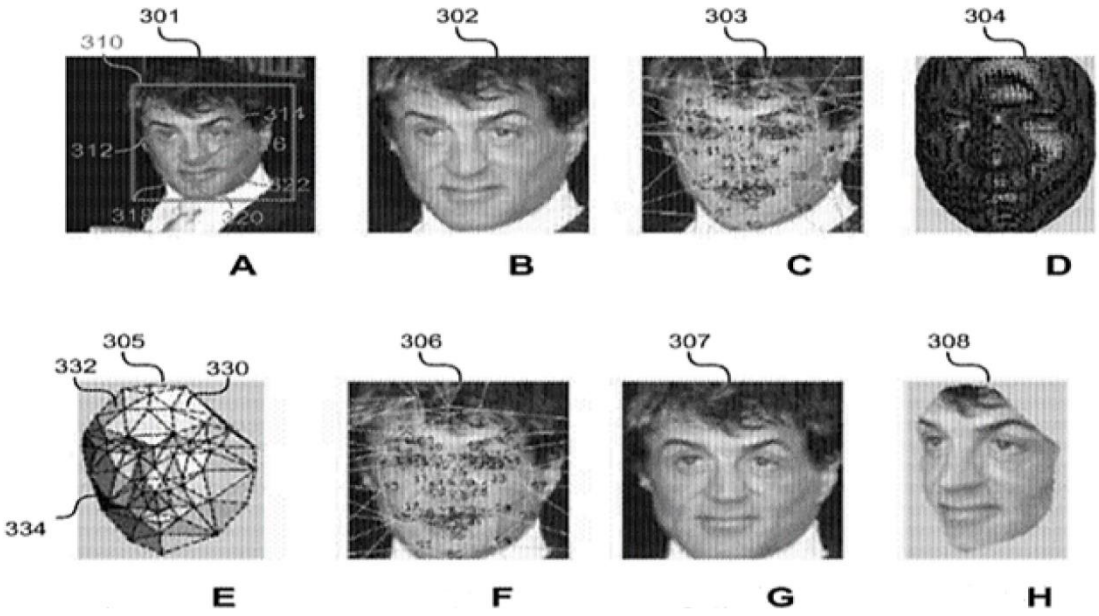


Figure 8. *Generate a 3D-aligned face image from a 2D face image. The steps from (A–H).*

3.4 Face Recognition Application Using Fog and Cloud Computing Technologies

Face recognition is now widely accessible through mobile smartphone applications. The smartphone user simply takes a photo of their own face or another person's face, and the application sends this image to a remote server hosted on either a fog or cloud platform. The server compares the image against a locally stored database of facial photos to identify the person depicted. This type of application has become very popular.

In an experiment described in [75], the smartphone application captures photos at a resolution of 384 × 286 pixels. The remote server's facial photo database contains 1,521 images, each also sized at 384 × 286 pixels. The experiment runs identical face recognition tasks on both fog computing infrastructure and Amazon Cloud EC2.

The authors report the following timing results for face recognition and response:

- Fog computing: face recognition time of 2.479 milliseconds (ms), and response time of 168.769 ms.

- Cloud computing: face recognition time of 2.492 ms, and response time of 899.970 ms.

Here, response time is defined as the interval from when the smartphone begins uploading the face photo until it receives the recognition result from the remote server.

Both fog and cloud platforms use virtual machines (VMs) with similar computational capabilities, resulting in comparable computation times for face recognition (around 2.5 ms in both cases). However, as Tables 2 and 3 indicate, the latency difference between fog and cloud in data transmission is small (less than 10 ms). This suggests that the large disparity in response time (approximately 731 ms) is mainly due to differences in network bandwidth.

Assuming negligible upload time in the fog scenario, the authors estimate that the smartphone uploads about 167 KB of data to the cloud within 731.201 ms. This is consistent with the average size of face photos uploaded, which is around 110 KB [75].

	RTT (ms)	Up/Down-Link Bandwidth (Mbps)
Fog	1.416	83.723/101.918
Cloud	17.989	1.785/1.746

Table 2. *Latency and Bandwidth Comparison.*

	Pre-Transmission Time (s)	Transmission Time (s)	Post_Transmission Time (s)
Full	207.050	143.694	43.982
Incremental	325.116	70.837	63.239

Table 3. *Fog VM Migration Performance.*

3.5 Human Silhouette/Figure Recognition System

Human identification can be achieved through video stream data classification methods. Besides Deep Learning, techniques such as Support Vector Machines (SVM), decision trees, and Bayesian classifiers are also used to determine precise human body positions. However, Deep Learning achieves near-perfect accuracy, recognizing human body positions with up to 100% accuracy, compared to other methods that reach around 93.72%.

The system identifies three primary human positions: standing, sitting, and lying down. To do this, it first receives input in the form of 20 human joint position

vectors. Using these inputs, the machine classifies the body's position. The data is captured using a Kinect camera positioned approximately two to three meters from the person.

Looking ahead, this technology is expected to serve as a foundation for analyzing time series of human body position sequences, enabling advanced applications such as motion analysis and fall detection within intelligent home systems [76].

CHAPTER 4

Smart-Home Ecosystem

This section presents the various IoT devices commonly found in smart home systems.

4.1 IoT in Smart Homes

As i showed, at my work, Vardakis G. et. al. “Review of Smart-Home Security Using the Internet of Things”, a typical smart home comprises multiple IoT devices interconnected via a central router-modem. This router functions as the primary network device, enabling communication among local devices at the edge and with external networks such as the Internet and cloud services. Most home devices do not maintain independent Internet connections; instead, the user interacts with the smart home ecosystem through a smartphone, which typically has a direct broadband connection. The router often serves as the sole barrier between the internal network and the outside world, making its security and configuration critically important.

Devices connect to the Local Area Network (LAN) created by the router either via Ethernet or wirelessly. Some may also establish direct connections with the user’s smartphone using technologies such as Bluetooth. These devices may expose services and APIs either locally within the edge system or externally over the Internet—therefore, securing and correctly configuring these interfaces is essential.

In modern configurations, home assistants (e.g., Amazon Echo, Google Nest) serve as key hubs for coordinating IoT devices. These assistants connect to the Internet via the router and wirelessly manage communication with local smart devices. The user controls the system using a smartphone, tablet, or PC, all of which connect to the home assistant either wired or wirelessly, while routine interactions are often carried out through voice commands.

Home assistants are among the most intelligent and versatile smart-home devices in modern installations [44]. They are often deployed to control less sophisticated devices, such as lighting and audio systems, and can store or access information about residents’ preferences and personal data. As a primary interface for user interaction, they allow voice-command control of the smart-home ecosystem without the need for a smartphone or other external device. Due to their central role and access to sensitive information, home assistants have become prime targets for advanced cyberattacks [77].

Popular home assistants like Google Home and Amazon Alexa are vulnerable to various threats, including voice squatting—where malicious actors exploit phonetically similar commands to trigger unintended actions [78,79]—and eavesdropping, where devices can be misused to capture private conversations. Additionally, these platforms have been targeted by malicious third-party applications and phishing attacks, posing risks to users' privacy and system integrity. As the adoption of such devices increases, attackers continue to explore new vulnerabilities to exploit [80,81].

Smart TVs are another common element in modern households [82]. They receive conventional television signals via antenna or cable and connect to the Internet (via wired or wireless router) for access to smart content. User interaction typically occurs via RF-based remote controls or through voice commands via an integrated virtual assistant or an external home assistant [45]. Many smart TVs are equipped with built-in microphones and cameras, enabling direct interaction through voice or gestures, and support peripheral connections like keyboards or mice via Bluetooth. Moreover, users often link personal accounts (e.g., YouTube, Netflix, or social media), which can create privacy concerns, especially when multiple household members or guests use the same device. This shared usage may inadvertently expose the owner's data and amplify potential security risks [83–86].

Augmented Reality (AR) and Virtual Reality (VR) glasses [46] represent another category of smart devices that may be found in modern home environments. These headsets typically connect wirelessly (e.g., via Wi-Fi) to the Internet through the home router. Users often log into social media or streaming platforms (such as Facebook or Netflix), raising similar privacy and security concerns as those associated with smart TVs. As with home assistants and smart TVs, malicious applications may be present in AR/VR app stores, potentially compromising the user’s data or device.

In the case of AR glasses, users interact with augmented environments during daily activities, including remote work. In such contexts—e.g., in a home-based augmented office—the glasses’ cameras may inadvertently capture sensitive on-screen information, such as login credentials, documents, or confidential conversations. This raises significant concerns about data privacy and workplace security. Moreover, due to their portable nature, AR/VR glasses are susceptible to loss or theft, particularly when taken outside the home. Consequently, enhanced device-level security mechanisms—such as remote data wipe, device locking, or secure user authentication—are essential to mitigate potential threats.

Smart locks are another increasingly common component of intelligent home systems, typically installed on doors and windows to control physical access [87]. These locks may operate via traditional mechanical means or through magnetic/electronic systems. For safety reasons (e.g., in case of fire, power outage, or Internet disruption), most smart locks allow for free exit from the inside. Entry into the home can be managed in various ways, including:

- Remote control via mobile applications,
- Wireless challenge–response authentication protocols with smartphones,
- PIN code entry on a keypad,
- Biometric verification (e.g., fingerprint or facial recognition),
- RFID cards or other access tokens,
- Or fallback physical keys, ensuring redundancy and reliability.

Smart locks are particularly popular in short-term rental accommodations, such as Airbnb or Booking.com properties. In these contexts, property owners can generate unique access credentials for each guest, as well as for service personnel like cleaners or maintenance staff. In contrast, hotels and cruise ships typically utilize magnetic card-based access systems, which offer centralized control and ease of management over room access.

The security of smart locks is critical, given that they control physical access to private spaces. Common attack vectors include exploiting communication protocol vulnerabilities, tampering with the hardware, bypassing biometric authentication mechanisms, or employing social engineering techniques to obtain access credentials.

Another widely adopted smart home component is the surveillance IP camera [88]. These devices are connected to the Internet through the home router (via Ethernet or Wi-Fi) and are often accessible remotely via a smartphone app. Cameras typically support bidirectional communication—allowing users not only to view live video and audio feeds, but also to remotely control the camera's orientation or speak through its built-in speaker. However, many users install these systems themselves and neglect to change default configurations, such as usernames and passwords [12]. This creates serious vulnerabilities, enabling attackers to:

Monitor whether the home is unoccupied, record private activities of the residents, violate privacy, or even interact with children in disturbing ways (e.g., by speaking through the camera).

Smart vacuums represent an early form of domestic robotics [89]. These devices operate autonomously to scan and clean indoor areas and can be remotely controlled

via RF remotes, smartphone apps, or Internet-based services. Through their mobile applications, users can schedule cleaning sessions, view historical data, or even access generated maps of their home layout. Some advanced models include camera sensors for navigation and obstacle avoidance. However, this capability also introduces privacy concerns, as these cameras may inadvertently capture sensitive information, such as the interior layout and the behavior of household members.

Other common smart-home devices and sensors include:

Smart lighting systems [90], which adjust ambient light based on user preferences or environmental cues,

Smart thermostats [91] and air conditioning systems [92], which control indoor temperature and energy consumption,

Smart ovens [93] and refrigerators [94], which monitor cooking and food storage and assist with shopping routines,

Smart plugs [95], which connect conventional appliances to the smart ecosystem, allowing for remote power control and automation.

Most of these devices are managed via smartphone apps, and once deployed, they are seldom updated or monitored for cybersecurity hygiene. This creates an environment where compromised devices can remain infected for extended periods without user awareness, potentially being exploited for cryptojacking or participating in Distributed Denial of Service (DDoS) attacks [96,97]. Moreover, these vulnerabilities can lead to serious consequences for the residents, including threats to physical safety, privacy breaches, and economic losses (e.g., due to excessive energy consumption or damaged appliances).

The disposal of smart-home devices introduces additional security and privacy challenges [98]. Many of these devices store sensitive user data. If not properly erased before disposal, this data can be recovered by malicious actors. The problem is exacerbated by the lack of clear and user-friendly procedures for securely wiping data and deregistering devices from associated user accounts or networks. Improperly disposed devices may retain the ability to connect back to the user's network, granting unauthorized access to ongoing live data or resources.

The same risks apply when devices are resold or transferred to new users. Consequently, robust data sanitization practices and secure decommissioning guidelines are essential.

Although the home resident is usually the primary installer and user of the smart-home system [99], they often lack the technical knowledge required to configure and

secure it adequately. Enhancing user awareness and digital literacy is therefore crucial. Additionally, others—such as guests (who gain temporary access to the home network) and technicians (who install or maintain equipment)—may interact with the smart environment. In shared spaces, such as rental properties or hotels, the residents themselves and the supporting staff may change frequently, further complicating secure system management and increasing the attack surface.

4.2 Infotainment Devices

Leading home assistant platforms, such as Google Home, Amazon Alexa, Apple Siri, and Microsoft Cortana, offer user-friendly interfaces and seamless integration with a wide range of smart-home devices [100]. These systems rely heavily on Deep Neural Networks (DNNs) and multimodal dialogue systems, encompassing Automatic Speech Recognition (ASR), Natural Language Understanding (NLU), and input from gestures and visual cues, thereby creating rich and immersive user experiences.

Despite their convenience, smart assistants raise significant concerns regarding privacy and cybersecurity. According to Fruchter and Liccardi [101], although only 2% of users explicitly report issues, concerns include extensive data collection, unexpected device behavior, and privacy intrusions. In the literature, a range of vulnerabilities has been identified [102–107], which include:

1. Continuous data collection and potential exposure to service providers or malicious actors.
2. Insecure data transmission or storage mechanisms, exemplified by Bluetooth-based attacks where adversaries can play voice commands from outside the home [108].
3. Third-party application vulnerabilities, due to inadequate vetting and permission management.
4. User misconfiguration and low security awareness, including weak authentication and lack of updates.
5. Exploitation of voice interfaces, through replay attacks, inaudible commands, or unauthorized vocal interactions.
6. Multi-user management challenges, particularly in shared environments or households with vulnerable users.
7. Account compromise, potentially exposing linked services and sensitive user information due to weak or reused credentials.

The always-on nature of these assistants amplifies privacy risks. Devices may inadvertently record conversations due to false wake-word detection, and such recordings are often processed and stored on remote servers. If these systems are compromised, attackers may gain access to a wealth of sensitive data, including contacts, calendars, financial information, and control over connected IoT devices such as smart locks, thermostats, and cameras.

Furthermore, third-party skills (e.g., via app stores) introduce additional attack surfaces. Malicious or poorly implemented skills can leak personal data or perform unauthorized actions. The dependency on regular security updates, often neglected by users or discontinued by vendors, further exacerbates these issues.

To mitigate these threats, a combination of user-level precautions and manufacturer responsibilities is required [103,109]. Recommended measures include:

- Enforcing strong and unique passwords,
- Enabling two-factor authentication,
- Applying security patches and firmware updates regularly,
- Monitoring permissions granted to third-party applications,
- Developing robust voice-based user authentication,
- Designing effective multi-user access control policies (e.g., distinguishing between adult and child privileges).

Smart TVs: Expanding the Attack Surface of the Smart Home

Smart TVs have evolved into central hubs of the smart-home ecosystem, combining traditional television with advanced connectivity and interactive capabilities. These devices support streaming services, smart-home integrations, voice commands, and third-party applications, leveraging sophisticated hardware and operating systems (typically Android or Linux-based) [82].

However, this increased functionality also brings a broad spectrum of cybersecurity threats [83–86]:

1. Remote exploitation via network vulnerabilities,
2. Malware/ransomware infections targeting the OS and applications,
3. Data interception, including credentials and viewing habits,
4. Physical attacks, such as malware injection via USB ports,
5. Third-party application vulnerabilities.

Particularly alarming are attacks that target the device's camera and microphone, allowing unauthorized surveillance. Additionally, because smart TVs often interface with other IoT devices, their compromise can provide a gateway to the broader home network.

To enhance security, several countermeasures have been proposed [84,86], including:

- Strong encryption protocols for data communication,
- Use of multi-factor or biometric authentication,
- Regular firmware and application updates,
- Implementation of secure boot and Trusted Execution Environments (TEE),
- Integration of AI/ML algorithms for anomaly detection,
- Adoption of privacy-enhancing techniques, such as differential privacy.

AR/VR Technologies in Smart Homes: Emerging Risks and Protections

The integration of Augmented Reality (AR) and Virtual Reality (VR) technologies into smart homes is transforming user interaction, offering immersive experiences and enhanced environmental control [46]. However, these technologies bring with them a new wave of privacy and security challenges [110–114].

AR/VR systems often collect:

- Real-time location data,
- Biometric data (e.g., gaze tracking, head movements),

- Visual/audio recordings of the home environment.

If compromised, these data can facilitate identity theft, surveillance, or social engineering attacks. Traditional password-based authentication is inadequate for AR/VR contexts. Instead, novel approaches—such as gesture-based access, eye-tracking, and behavioral biometrics—have been explored [113]. Yet, even these techniques may be vulnerable to spoofing or replay attacks.

Additionally, AR/VR devices are typically connected to the home's main network, increasing the risk of cross-device compromise. Insecure or malicious applications may exploit motion sensors, voice inputs, or embedded cameras, capturing data or issuing commands without user consent.

Mitigation strategies include:

- Use of end-to-end encryption for AR/VR data streams,
- Deployment of edge computing to minimize cloud dependencies,
- Implementation of privacy-by-design principles,
- Periodic security audits and automatic updates,
- Enforcing local authentication using multiple biometric and contextual cues.

4.3 Physical Home Security and Monitoring

Smart locks, an integral component of the modern smart-home ecosystem, represent a significant evolution from traditional mechanical locks to digitally operated systems [87]. These devices enable users to lock and unlock doors via smartphones, voice commands, or even remotely through Internet connections. While the convenience and enhanced functionality of smart locks are undeniable, these features also introduce a range of security vulnerabilities, potentially exposing users to unauthorized access and data breaches.

The core appeal of smart locks lies in their connectivity, which allows users to control access to their homes from virtually anywhere. However, this convenience also creates multiple attack vectors for cybercriminals [115]. Most smart locks connect to home networks via Wi-Fi or Bluetooth, and weaknesses in these communication protocols can be exploited. For instance, flaws in Bluetooth security—such as weak pairing mechanisms or protocol vulnerabilities—can enable attackers to intercept communications and gain unauthorized access to the lock.

Moreover, many smart locks are integrated into broader home automation platforms that collect and store personal data [116]. Consequently, compromising a smart lock could provide a gateway to other connected systems, such as surveillance cameras or personal devices, amplifying the impact of a breach. The risk is further heightened by poor user practices, such as failing to change default passwords or implement strong authentication mechanisms.

To address these issues, researchers are exploring innovative solutions, including the use of blockchain technology to develop decentralized access control systems, thereby avoiding single points of failure [117,118]. In parallel, Machine Learning (ML) is being leveraged to develop intelligent threat detection systems that can recognize and respond to anomalous behavior in real time by learning from historical usage patterns [119].

Manufacturers have responded by adopting multiple security-enhancing strategies [116]. These include the implementation of advanced encryption protocols such as the Advanced Encryption Standard (AES), which ensures secure communication between smart locks and user devices. Additional features like geofencing—which automatically locks or unlocks doors based on the user's GPS-determined location—further enhance security and usability.

Ultimately, securing smart locks is a multifaceted challenge requiring both technological advancement and user education [120]. Users must adopt best practices, including using strong, unique passwords, enabling two-factor authentication, and regularly updating device firmware to protect against emerging threats.

The integration of surveillance cameras into smart homes significantly enhances security but also introduces unique vulnerabilities [88]. These cameras, central to modern home security, are capable of recording high-resolution video and interfacing with other smart systems. However, their connectivity also makes them targets for cyber-attacks [121].

One of the primary concerns is their susceptibility to hacking. Cybercriminals can gain remote access to cameras through unsecured networks or by exploiting firmware vulnerabilities [122]. Once compromised, attackers can disable the cameras, alter recordings, or conduct covert surveillance. This poses serious privacy concerns, as intercepted footage may reveal sensitive personal routines and private household activities [123,124].

To mitigate these risks, encryption of data streams and secure storage of footage are critical. Moreover, advanced ML algorithms are being deployed to analyze video

feeds, differentiate between routine and suspicious activity, and support intelligent threat detection [125]. These systems can recognize intruders even in low-light conditions or when facial features are obscured. However, they also increase system complexity and may lead to false positives or privacy concerns if mishandled.

Effective mitigation strategies include enhancing the physical security of the camera—such as implementing tamper-detection mechanisms—and improving encryption during data transmission [122]. Regular firmware updates and robust authentication protocols are essential for maintaining the integrity of these systems.

Future research should focus on developing resilient ML models that balance accuracy with privacy preservation. Additionally, the establishment of comprehensive data governance frameworks is necessary to regulate the collection, processing, and sharing of user data. Such frameworks would help ensure that personal information is accessed only under strict, clearly defined conditions. As smart-home technologies become more integrated and complex, adopting a holistic and proactive security approach will be critical to maintaining user trust and system resilience.

4.4 Ambient Living Devices

4.4.1 Security Challenges in Smart Vacuums and Other Smart-Home Devices

Smart vacuum robots [89], as integral components of the smart-home environment, have evolved beyond their traditional cleaning roles to incorporate IoT-enabled functionalities such as mapping household layouts, scheduling cleanings, and remote operation via smartphone applications. However, as these devices become more deeply embedded in personal spaces, the associated security risks are correspondingly magnified.

A major security concern lies in their connectivity to the home network. If compromised, smart vacuums can serve as an entry point for attackers to infiltrate other connected systems. This threat is exacerbated by the fact that many smart vacuums run on common operating systems, such as Linux, making them vulnerable to known exploits. Researchers have demonstrated that vulnerabilities in vacuum firmware can be exploited to gain root access, enabling attackers to control the device, map the interior of homes, or even repurpose the device as a listening tool [126].

Another significant threat concerns the data collected by these devices. Smart vacuums generate detailed spatial maps of homes [127], and if this data is intercepted or mishandled, it could pose serious privacy violations. Notably, some studies suggest that lidar sensors on smart vacuums can be manipulated to capture audio information by analyzing object vibrations—revealing a novel attack vector whereby benign household devices can be transformed into surveillance tools.

Furthermore, the integration of smart vacuums with cloud platforms—for functionalities like remote access and firmware updates—introduces additional vulnerabilities. Without proper encryption and secure data management, the information transmitted between the vacuum and the cloud is susceptible to interception. The reliance on mobile applications also broadens the attack surface, as poorly designed apps can expose user credentials or allow unauthorized control over the devices.

To mitigate these threats, manufacturers must adopt comprehensive security measures. These include securing communication with end-to-end encryption, implementing strong authentication mechanisms, and ensuring frequent firmware updates. Future research should explore the development of real-time intrusion detection systems, enhanced data privacy protocols, and the application of blockchain and decentralized architectures to ensure secure device communication and data integrity.

4.4.2 Broader IoT Device Vulnerabilities in Smart Homes

The proliferation of smart vacuums and other IoT devices presents a complex array of security challenges. Ensuring that these devices do not compromise the environments they are designed to enhance requires a multi-layered security strategy. The wider landscape of smart-home devices—including smart lighting, thermostats, air-conditioning units, ovens, fridges, and smart plugs—offers considerable convenience but also introduces significant risks.

Smart lighting systems offer features such as remote control, scheduling, and adaptive lighting based on occupancy or ambient light levels [90]. However, their network connectivity makes them vulnerable to attacks. A compromised lighting system could not only disrupt household routines but also serve as a gateway to more sensitive devices.

Smart thermostats, which adjust environmental conditions based on user behavior and preferences, present similar concerns [91]. These devices gather detailed information about user presence and daily routines, which could be exploited by intruders to plan burglaries or by malicious actors to craft targeted attacks. If compromised, thermostats can also cause environmental harm or energy wastage through extreme temperature changes.

Smart air-conditioning systems, increasingly integrated into smart ecosystems, face the same threats [92]. Unauthorized control can lead to user discomfort, increased energy bills, or potentially serve as an entry point to more critical parts of the smart-home network.

Smart ovens and refrigerators introduce more direct physical safety concerns [93,94]. For example, a hacked oven could be turned on remotely, posing fire hazards, while smart fridges—connected to online grocery services and storing dietary data—could be used to access personal information or disrupt food storage, leading to health risks.

Smart plugs, which control power to other devices and monitor energy consumption, may appear benign but can be weaponized [95]. If compromised, they could disable essential equipment such as medical devices, security systems, or refrigeration units, resulting in severe consequences.

4.4.3 Mitigation Strategies and Future Directions

To address these vulnerabilities, robust security practices are essential [96,97]. These include:

- Using strong, unique passwords
- Encrypting communications to prevent data interception
- Regular firmware updates to patch known vulnerabilities
- Ensuring devices include physical tamper resistance
- Following secure mobile app development practices

In addition, network segmentation can significantly enhance security by isolating smart devices into separate sub-networks. This architectural strategy ensures that, even if one device is compromised, the breach does not automatically propagate to others or to sensitive personal data in the main computing environment.

Manufacturers must prioritize security-by-design principles, embedding protections into every layer—from hardware to firmware and user interfaces. Users, too, play a vital role and should be educated on best practices to ensure the integrity of their smart-home environments.

As the smart-home ecosystem continues to expand, interdisciplinary research and regulation will be crucial to developing resilient and privacy-preserving frameworks that adapt to emerging threats while maintaining the convenience and efficiency these devices promise.

4.5 Other Aspects and Actuators

Smart-home security extends beyond the technological vulnerabilities of devices; it encompasses human factors, user awareness, device management, disposal practices, regulatory standards, and manufacturers' responsibilities [98,99]. Addressing these dimensions is essential to establishing a resilient and trustworthy smart-home ecosystem.

Human Factors and User Awareness

The human factor is a critical component of smart-home security [99]. A significant proportion of users remain unaware of the threats posed by smart devices and the

practices needed to mitigate them. For instance, many users fail to change default passwords, leaving their devices vulnerable to brute-force attacks. Additionally, the growing prevalence of voice-activated systems introduces new privacy risks; voice assistants may inadvertently record or transmit private conversations, often without explicit user consent.

To mitigate these risks, user education is imperative. Consumers should be informed about:

- The importance of securing home Wi-Fi networks (e.g., using WPA3, hiding SSID, restricting MAC addresses).
- Recognizing social engineering and phishing attacks targeting device credentials.
- Regularly checking and updating device security settings and firmware.

Promoting awareness about safe installation and maintenance practices, along with the consequences of careless device usage, is a foundational step in enhancing smart-home security.

Device Management and Disposal

Management and disposal of smart-home devices also raise important security concerns [98]. Proper device management includes the regular installation of software and firmware updates, which are crucial for patching known vulnerabilities. Yet many users neglect or are unaware of this maintenance responsibility, creating prolonged exposure to exploitable flaws.

Device disposal presents further risks. Devices such as smart thermostats or virtual assistants may retain sensitive data even after disconnection. Without proper sanitization (e.g., factory resets, data deletion procedures), discarded devices could be exploited by malicious actors to extract personal information.

To counter this, manufacturers and retailers should:

- Provide clear instructions on how to wipe data prior to disposal.
- Encourage recycling programs with built-in secure erasure processes.
- Inform consumers about the security risks of second-hand device markets.

Manufacturers' Responsibilities

Manufacturers play a central role in establishing secure smart-home ecosystems [103,109,116]. Security must be embedded from the design stage, incorporating:

- Strong encryption standards for data transmission and storage.
- Secure authentication protocols, such as two-factor authentication.
- Tamper-resistant hardware to prevent physical exploitation.

In addition to design security, long-term support for devices is critical. This includes issuing timely security patches, disclosing known vulnerabilities, and providing emergency responses to active threats. Transparency and proactive communication can build consumer trust and contribute to a safer digital environment.

Furthermore, simplifying device usability is key. Manufacturers should:

- Develop intuitive interfaces for monitoring and updating security settings.
- Implement security-by-default principles, such as mandatory password changes on first use or automatic firmware updates.
- Provide real-time alerts about potential threats, such as suspicious access attempts or outdated software.

By reducing the technical burden on users, manufacturers can make secure behavior the default choice, rather than a user-dependent decision.

Standardization and Regulation

One of the persistent challenges in securing smart-home environments is the lack of universal security standards for IoT devices [128–133]. Regulatory fragmentation across countries results in inconsistent practices and compliance burdens for manufacturers, complicating efforts to deliver secure products globally.

The development of comprehensive international standards would streamline security implementation and enforcement. These standards should define:

- Baseline security requirements for all IoT devices.
- Data protection frameworks compatible across jurisdictions.
- Security certification processes to help consumers make informed purchasing decisions.

Such initiatives would not only support manufacturers but also empower consumers to evaluate and compare the security posture of different smart-home products before integration into their personal spaces.

CHAPTER 5

Analysis of the IoT Setting

5.1 Architectural Structure of IoT Ecosystems

To effectively study the security of a smart-home environment utilizing IoT technology, it is essential to first establish a clear understanding of its architectural structure. Typically, IoT devices communicate within the edge system, either directly or via a gateway, and may also interact with external systems through the Internet or cloud-based platforms. The structure of an IoT architecture is not universally standardized; rather, it is informed by a combination of industry best practices, architectural principles, and the recommendations of various standardization bodies.

Several organizations have developed frameworks and guidelines that, while not prescribing a single architecture, serve as foundational references for IoT system design:

- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC): ISO/IEC 30141 [128] provides architectural reference models and interoperability principles for IoT systems. Although it does not explicitly define distinct layers, it lays out core design principles for scalable and interoperable solutions.
- Institute of Electrical and Electronics Engineers (IEEE): IEEE P2413 [129] outlines a high-level architectural framework for IoT, addressing aspects such as cross-domain interactions, security, and interoperability, albeit without prescribing a strict layer-based structure.
- Industrial Internet Consortium (IIC): The Industrial Internet Reference Architecture (IIRA) [130] provides a detailed and modular approach to designing industrial IoT (IIoT) solutions. Despite its industrial focus, its layered concepts and system views are adaptable to broader IoT domains.
- Open Connectivity Foundation (OCF): The OCF focuses primarily on interoperability protocols and device connectivity standards [131], offering architectural principles that support seamless integration and communication among heterogeneous IoT devices.
- National Institute of Standards and Technology (NIST): NIST contributes significantly to IoT security frameworks through documents such as the

Cybersecurity Framework and Special Publication 800-183 [132,133], which address system-level security concerns and architecture design principles.

Although no unified standard exists for defining IoT architectural layers, these frameworks collectively support the development of secure, scalable, and interoperable IoT solutions.

Conceptual Layers in IoT Architecture

Based on established frameworks and current research (e.g., [22]), a widely accepted conceptual model in IoT studies includes four primary layers:

1. Application Layer – responsible for delivering IoT services (e.g., smart homes, cities, or healthcare systems);
2. Perception Layer – incorporates sensing technologies such as motion, smoke, and pressure sensors;
3. Network Layer – manages data routing, transmission protocols, and communication topologies;
4. Physical Layer – includes the hardware components enabling connectivity and data acquisition.

These layers are discussed in further detail below.

Application Layer

The application layer [134] is the topmost layer in the IoT architecture and governs the execution of IoT applications in various domains, including smart homes, smart cities, healthcare, and transportation. It ensures that applications can interact with users and with lower architectural layers, facilitating the deployment of services tailored to user needs.

This layer plays a pivotal role in maintaining the confidentiality, integrity, and availability (CIA) of data and applications. It also handles authentication mechanisms and user access rights. However, it remains highly susceptible to attacks, particularly through malicious applications, insecure APIs, or vulnerable device firmware [134]. Effective security mechanisms at this layer are thus essential to prevent data breaches and unauthorized control over IoT devices.

Perception Layer

Often referred to as the sensing layer, the perception layer consists of sensors and technologies that collect data from the environment. This includes devices such as

pressure sensors, RFID readers, vibration detectors, and smoke sensors. It serves as the interface between the physical world and the digital network, capturing data necessary for intelligent system behavior.

A core challenge of this layer is the efficient and accurate collection of data under variable environmental and operating conditions [135]. Additionally, this layer is exposed to physical tampering and data manipulation threats, making sensor integrity verification a key security concern.

Network Layer

The network layer [136] acts as the communication backbone of the IoT system. Its primary responsibility is to transmit data collected from the perception layer to application servers or cloud platforms. It supports both wired and wireless communication protocols, facilitating connectivity between terminal nodes (e.g., sensors) and processing units (e.g., edge servers or data centers).

This layer is critical in supporting real-time data transmission, routing protocols, network topologies, and device addressing schemes. It is also the focal point for many cybersecurity threats, such as eavesdropping, packet injection, and denial-of-service (DoS) attacks. Security mechanisms in this layer should include strong encryption, network segmentation, and intrusion detection systems to prevent unauthorized data access and traffic manipulation.

Physical Layer

The physical layer [137] encompasses all hardware components involved in a smart environment. This includes end-user devices such as smartphones, smartwatches, tablets, smart TVs, locks, fridges, and smoke detectors, as well as network hardware like routers, switches, and gateways.

This layer provides the physical connectivity and serves as the foundational platform upon which the perception layer operates. It also includes power supplies and embedded processors, making it susceptible to threats such as physical tampering, unauthorized device replacement, or energy-depletion attacks.

Securing the physical layer involves implementing tamper-resistant designs, secure boot mechanisms, and device authentication protocols that prevent unauthorized hardware integration.

Understanding the layered structure of IoT systems is fundamental to identifying and mitigating security risks in smart-home environments. Although no

universal framework exists, various standards and best practices guide the implementation of robust, flexible, and secure architectures tailored to the diverse applications of IoT.

5.2 Threats Faced by a Smart Home and Related Countermeasures

As the number of Internet-connected devices supporting IoT technology continues to increase, prioritizing security measures within these systems becomes essential [138]. This urgency is amplified in smart-home environments, where IoT devices are responsible for safeguarding homes against intrusions and managing critical emergency responses such as fire or smoke detection. Typically, smart-home devices connect to the Internet through a gateway, which acts as an intermediary between the local network and the wider Internet. To ensure the security of such smart-home systems, it is vital to implement robust security protocols across every layer of the IoT architecture (see Figure 9).

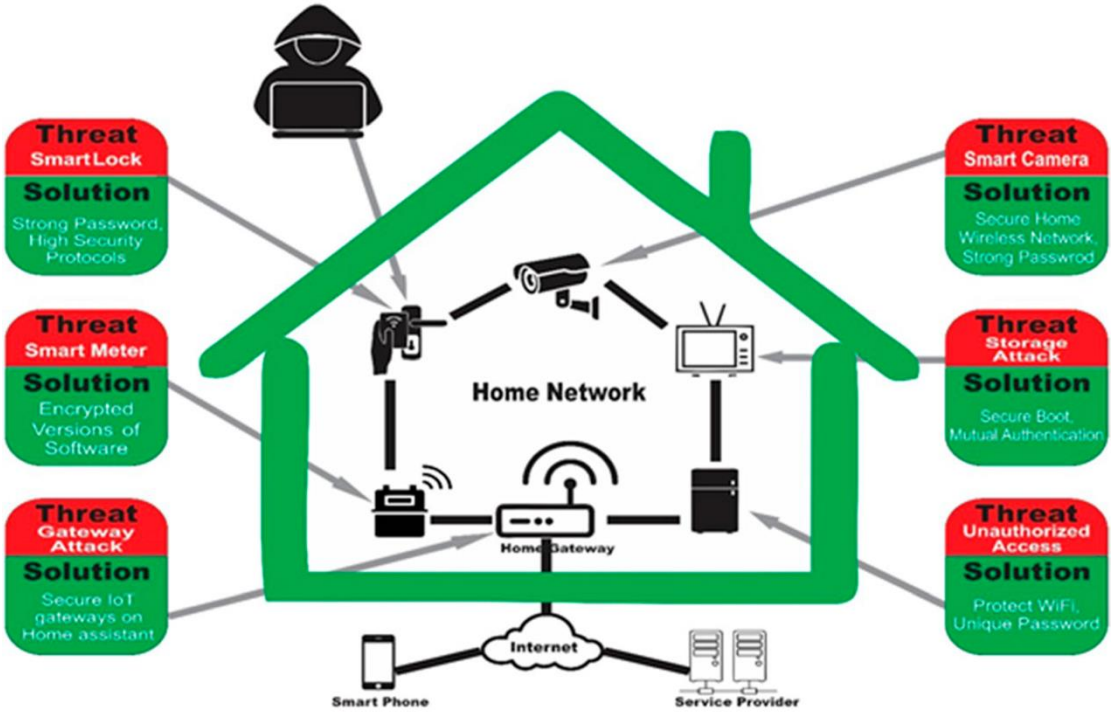


Figure 9. *Smart-home threats and countermeasures* [33].

Below, we present and analyze the types of attacks that can target each architectural layer individually, along with the corresponding countermeasures and controls designed to mitigate these threats.

5.2.1 Application Layer Analysis

Attacks targeting the application layer can cause malfunction or disruption of services, severely impacting the smart-home environment. Among these, social engineering attacks are particularly common, where attackers manipulate legitimate users or administrators to reveal sensitive access credentials [139,140]. Phishing attacks, a subtype of social engineering, involve deceptive emails or fake websites designed to steal passwords. Another common attack vector involves tricking users into installing malware disguised as legitimate software, granting attackers full access to the system's data and control [138,141–144]. Such malware can target devices connected to the Internet, often leading to total system compromise or crashes.

Malicious software (malware)—including worms and ransomware—is frequently used to infiltrate IoT devices. Worms can spread across various operating systems (including Linux), and smart-home devices like cameras and routers are frequent targets, as seen in the infamous Mirai botnet attack [42,145–148]. Ransomware encrypts user data and demands payment, severely affecting the application and network layers. Additionally, crypto-jacking exploits a device's processing power to mine cryptocurrency without user consent, degrading device performance and increasing energy costs.

Attacks on nodes often involve installing rootkits to gain unauthorized control, causing devices to behave abnormally or impersonate legitimate users—commonly known as access control attacks [149–153]. Unlike traditional computers, many smart devices lack automatic security updates; when updates occur, they can temporarily disable encryption, opening a window for attacks [154–157]. Moreover, unauthorized software from untrusted developers can introduce vulnerabilities, especially since many IoT devices use default settings without strong authentication, allowing attackers easy access [158,159].

Smart-home IoT systems rely heavily on remote communication with servers, raising concerns about unauthorized reconfiguration through the Internet [14,15,160]. Attackers exploiting weak protections can alter device settings to intercept or manipulate sensitive data.

Countermeasures and Best Practices

User Training and Awareness: Educating users and administrators about phishing and social engineering is crucial. Proper authentication protocols at the network level can also help prevent phishing attacks [18,143]. Abbas et al. [161]

propose a threat modeling approach using the STRIDE framework to identify and mitigate social engineering threats in IoT environments.

- Machine Learning (ML) for Phishing Detection: Several studies utilize ML techniques to detect phishing messages and classify incoming communications to block malicious attempts [162–165].
- Malware Detection Techniques: Dynamic analysis methods, such as Markov chain behavioral models of API calls [166], and hybrid detection techniques [167], help identify suspicious applications. Wang et al. [168] emphasize comprehensive feature extraction to improve ML accuracy in detecting malicious apps on Android devices.
- Authentication Protocols: Novel multi-factor authentication protocols for smart homes, including Elliptic Curve Cryptography (ECC), secret sharing, and biometric methods like Photo Response Non-Uniformity (PRNU) and face recognition, enhance security and user convenience [169,170].
- Rootkit Detection: Utilizing Trusted Execution Environments (TEEs) to isolate rootkit detection processes has been shown effective in preventing rootkits from interfering with system security [171].
- Update Management: User perceptions often underestimate the importance of updates for security. Research by Haney and Furman [172,173] highlights the need for better communication about update benefits, enhanced transparency, and more user-friendly update mechanisms to encourage timely application of security patches.

5.2.2 Perception Layer Analysis

The perception layer of an IoT architecture, responsible for sensing and data collection through embedded devices, is a frequent target for cyberattacks. Attackers exploit vulnerabilities at this level to intercept, modify, or reroute sensitive data. A common method involves manipulating the communication software of network nodes, enabling a malicious device to join the network and eavesdrop on transmitted data. This unauthorized access is particularly dangerous due to the typically weak security protocols governing device-to-server communication, often executed over the Internet without sufficient encryption. This type of breach is categorized as eavesdropping [174,175].

Another tactic involves the installation of sniffer applications on legitimate devices, enabling attackers to deactivate and subsequently reactivate the device with full access to its collected data [176]. Attackers may also target devices during their boot process—a period in which security protocols like UART and JTAG have not

yet been initialized. These boot attacks exploit the vulnerable startup state to gain system control [25,152].

Due to their low power consumption, many home IoT devices are physically and logically susceptible to tampering. Attackers can disable these devices and replace them with counterfeit ones that mimic expected behavior while secretly extracting data [176]. Additionally, side-channel attacks—such as timing, electromagnetic, and laser-based intrusions—exploit unintended physical emissions or timing discrepancies to extract sensitive information [152,177]. These attacks are made feasible by the low-power architecture and wireless nature of IoT sensors.

Another major challenge stems from network noise—irrelevant or corrupted data introduced by attackers that leads to sensor malfunction and erroneous data transmission. Such noise can disrupt service quality and system integrity [178–180].

Because sensors represent the first point of interaction in a smart-home IoT system, securing them is critical. Insecure sensors should not be exposed and must be housed in protected environments. To safeguard the perception layer, several protective strategies are proposed:

1. Private Network Deployment: IoT devices should operate within private, secured networks rather than public or open-access networks, which are more susceptible to intrusion. Attackers often create rogue networks mimicking legitimate ones to deceive users.
2. Secure Hardware and Software: Devices should employ encrypted software from certified developers and operate with trusted OEM hardware. This reduces the risk of device compromise through unauthorized firmware or counterfeit hardware.
3. Traffic Obfuscation Mechanisms: Abrishamchi et al. [181] introduce a hybrid energy-efficient privacy-preserving scheme to thwart wireless traffic sniffing. This model uses probabilistic algorithms to inject dummy packets and modify transmission schedules, thereby confusing potential eavesdroppers while maintaining energy efficiency.
4. Artificial Intelligence for Anomaly Detection: Xinchuan and Martinez [182] employ neural networks that learn normal operational patterns through continuous observation, enabling them to detect noise-induced anomalies and side-channel attacks in real time.
5. Cryptographic Protections: To prevent data leakage even in lossy transmission environments, Zhihua et al. [183] propose a leakage-resilient public key infrastructure (PKI) approach. This method ensures data confidentiality through robust encryption, even if some bits are lost during transmission.
6. Secure Boot Mechanisms: Yuan et al. [184] advocate for a secure boot process, including the encryption of the FPGA bitstream and system boot image. This prevents unauthorized access during startup and verifies system integrity through authentication procedures.

In summary, the perception layer, while foundational to IoT functionality, remains particularly vulnerable due to its exposure, resource constraints, and reliance on wireless communication. By integrating energy-efficient obfuscation methods, AI-based anomaly detection, strong encryption, and trusted boot protocols, smart-home systems can significantly enhance their resilience against perception-layer threats.

5.2.3 Network Layer Analysis

The network layer plays a critical role in managing device pairing, secure communication, and data routing in IoT systems. It authenticates devices and coordinates their interaction across the network. However, it is also a significant attack surface, vulnerable to several types of intrusions that can disrupt operations or compromise sensitive data.

Key Threats at the Network Layer

One of the most prominent attacks is the Denial of Service (DoS) attack, wherein an attacker floods the network with excessive data packets, overwhelming nodes and rendering them incapable of performing basic functions [159,185]. As a result, legitimate users are denied access, and attackers may exploit this congestion to infiltrate the network and alter device-pairing parameters, gaining unauthorized access to data flows.

Another significant vulnerability lies in the gateway, which acts as the bridge between smart devices and remote servers. In a gateway attack, the attacker compromises the routing mechanism, redirecting data through malicious nodes and severing the connection between sensors and the IoT backend (e.g., the cloud or ISP infrastructure) [180,186,187]. This may lead to total service disruption and acts as a precursor to DoS attacks.

Attacks that impersonate legitimate users can be particularly destructive, especially in domains such as smart healthcare, where the interception or modification of sensitive patient data can have severe consequences [22,188–190]. The increasing storage of personal information on local devices or in the cloud—often with broad user access—further exacerbates the system's vulnerability [191–193].

A more covert tactic involves the black-hole attack, where a malicious device silently intercepts all traffic by posing as a legitimate relay node. Without disrupting overall system performance, it siphons data from the network [35]. Similarly, man-in-the-middle (MITM) attacks involve intercepting communications between devices, often injecting irrelevant or harmful data that can mislead nodes and compromise system integrity [194,195].

A notable routing attack is the HELLO flooding attack, where a node bombards others with HELLO messages, falsely presenting itself as a nearby neighbor. This causes other nodes to accept it as a parent node and reroute traffic

through it, allowing the attacker to alter network routing paths [41]. The diversity of communication technologies used in smart environments introduces further vulnerabilities, making interoperability a double-edged sword in terms of security [152,178,195,196].

Countermeasures and Security Solutions

To defend against network-layer threats, a combination of proactive, reactive, and adaptive solutions is necessary:

- Network-based DoS Detection and Mitigation: ISPs often deploy mechanisms to detect DoS attacks early—such as traffic pattern analysis and filtering—to block malicious traffic before it reaches the end-user. End devices can also implement anti-DoS techniques, such as backoff algorithms, which delay responses under high traffic loads.
- Botnet Awareness and Response Systems: The WARDOG system is a user-centric security solution that mitigates botnet activity and DoS threats [197]. It alerts end-users of infections and enables infected devices to automatically block malicious activity. In addition, it gathers forensic data for potential legal action. WARDOG's compatibility with existing infrastructure, scalability, and zero-cost design make it ideal for widespread deployment.
- Multi-Factor Device Authentication: To prevent unauthorized access and MITM attacks, a secure multi-factor authentication scheme based on digital signatures and device capabilities has been proposed [198]. Devices must pass rigorous identity verification before network admission. The authentication server is also validated, and further access is governed by role- or attribute-based authorization.
- Attribute-Based Access Control: Ameer et al. [199] propose HABACα, an attribute-based access control (ABAC) model tailored for smart-home environments. This dynamic, fine-grained approach considers user roles, environmental factors, operations, and device characteristics to construct adaptive security policies that evolve with usage context.
- Secure Routing Systems: To counter routing and flooding attacks (such as HELLO floods), [200] introduced SCOTRES, a trust-based secure routing protocol for IoT and cyber–physical systems. It evaluates routing decisions using five metrics: energy consumption, topology awareness, channel health,

reputation, and trust. SCOTRES aims to balance load distribution, extend network lifetime, and improve resilience against jamming and misbehavior.

- Intrusion Detection and Prevention Systems (IDS/IPS): Rajora and Sharma [201] present TWINKLE, a lightweight IDS/IPS architecture for smart homes. TWINKLE operates in two modes:
    - Normal Mode conserves resources during regular operation.
    - Watchful Mode is activated upon anomaly detection, intensifying monitoring and defense mechanisms.

      TWINKLE reduces detection latency and resource usage, making it ideal for resource-constrained IoT environments, while effectively defending against DDoS and sinkhole attacks.

The network layer in smart environments is a critical yet vulnerable component of IoT systems. Attackers exploit communication protocols, routing strategies, and device access policies to intercept, redirect, or disrupt data flows. However, emerging security frameworks—including multi-factor authentication, intelligent routing, trust-based systems, and machine learning-based IDS—provide a strong foundation for robust network-layer defense. The integration of these tools not only protects sensitive data and ensures system availability but also preserves user trust and system longevity in evolving smart-home infrastructures.

5.2.4 Physical Layer Analysis

The physical layer of an IoT system encompasses all hardware components—smart devices, sensors, and communication interfaces—that enable connectivity and interaction with the Internet. This foundational layer is especially vulnerable to a range of environmental, hardware-based, and signal interference attacks that can severely impair system integrity.

Power Supply Vulnerabilities

The installation and continuity of an electrical power supply are critical building blocks for any smart environment. Power failure—whether due to environmental conditions or malicious intervention—can create critical points of failure [202,203]. Devices often lack backup energy sources and rely solely on the main power grid. As a result, during a power outage caused by natural disasters or deliberate sabotage, devices may shut down entirely or enter low-power mode, reducing their functionality and potentially sending incorrect or outdated data [204–207].

These power-related malfunctions constitute hardware failures that can escalate into network-wide failures, especially in systems where node dependency is high. Even the underperformance of a single device can compromise broader system operations.

Environmental and Jamming Attacks

Devices exposed to extreme weather phenomena, such as heavy rain or snow, are susceptible to damage and malfunction—known as environmental attacks [204,205]. These incidents reduce sensor accuracy and system responsiveness, particularly in outdoor deployments.

Another frequent threat to the physical layer is radio frequency (RF) jamming, where attackers transmit high-power signals to disrupt wireless communication [208]. Depending on the strength and proximity of the jamming signal, the network may experience partial or total collapse. Even in partial jamming, affected nodes must filter through noise and retransmit lost data, consuming significant power and amplifying the risk of full-system failure.

Malware Injection and Device Spoofing

Malware injection is another serious threat at the physical layer. Attackers may exploit debugging interfaces to inject malicious code into a network via spoofed devices. Once the malware is disseminated across the network, it enables unauthorized access to data or complete system shutdown [204].

In Radio Frequency Identification (RFID) systems, attackers can launch noise signal attacks that saturate the communication channel with irrelevant data. Since RFID components are generally low-power, such RF noise attacks render them incapable of properly transmitting tag data [36].

Perhaps more insidious is the device cloning attack, where an attacker creates a replica device mimicking a legitimate one—using identical hardware identifiers, software configurations, and manufacturer details [209,210]. These clone devices infiltrate the network, deceive RFID readers, and propagate malware to other nodes, compromising the system's confidentiality, integrity, and availability. The attacker can intercept or manipulate transmitted data, altering the system's behavior to suit malicious objectives [33,138,141,142].

Countermeasures at the Physical Layer

To mitigate the above risks, a range of technological and architectural solutions have been proposed:

- Environmental Resilience: Devices should be deployed in protected or controlled environments to reduce exposure to natural elements. Enclosures with weatherproofing or adaptive cooling/heating can significantly reduce weather-induced hardware failures.

- Cloning Detection via Hashing Mechanisms: One countermeasure against device cloning is the use of hashed double collisions. This method collects and analyzes duplicate hash values to detect tag replication and ensure data flow integrity.
- Quantum Key Distribution (QKD): Maninder and Sheetal Kalra [175] proposed a Quantum Key Distribution-based authentication scheme to reinforce mutual trust between users and servers. QKD uses quantum properties to generate secure cryptographic keys, offering resistance to eavesdropping, spoofing, and device cloning. The inherent unpredictability and non-replicability of quantum states make this approach exceptionally secure.
- Machine Learning-Based Detection: Jeyaselvi et al. [211] utilized Support Vector Machine (SVM) algorithms to detect cloning and jamming attacks in IoT sensor networks. Their method analyzes the distance metrics between nodes and the base station, classifying devices as normal or malicious. This ML-based approach increases the accuracy of anomaly detection and helps maintain robust network operation.
- Trust-Based RFID Authentication: Mbarek et al. [212] developed TRAS (Trust-Based RFID Authentication Scheme), which incorporates historical behavior—such as prior keys, transaction logs, and node capabilities—into the authentication process. TRAS dynamically evaluates RFID tag legitimacy, offering a more resilient defense against cloning and jamming attacks.

The physical layer of IoT environments is uniquely susceptible to a wide spectrum of threats, from power instability and environmental damage to RF jamming, malware injection, and device cloning. These vulnerabilities can lead to significant degradation or total collapse of smart systems, particularly in critical infrastructure like healthcare or smart cities.

To address these risks, security solutions must combine robust physical design with advanced detection mechanisms, cryptographic innovations like QKD, and trust-based authentication frameworks. Integrating machine learning for anomaly classification and implementing layered security at the hardware level can significantly enhance system resilience against physical-layer attacks.

5.2.5 Summary of Threats and Countermeasures

Table 4 summarizes the cyber threats for each IoT layer along with the indicative solutions and countermeasures.

Layer	Threats	Countermeasures
Application	Social-engineering and phishing	Threat modeling [154], ML detection [162,165], user training, and raising awareness [19,20]
	Installation of malicious software and applications	Code and application analysis [166-168]
	Attacks on access control	Multi-factor authentication [169], privacy preserving authentication [170]
	Rootkit attacks	Rootkit detection with TEE [171]
	Failure to install security patches and updates	User education [173]
Perception	Eavesdropping and sniffing attacks	Operate within private networks and transmission of fake packets protocol [181]
	Side-channel attacks	Encrypted communication [183]
	Noise in data	AI and neural network anomaly detection [182]
	Booting attacks	Secure booting with encryption and authentication [184]
Network	DoS	WARDOG device notification and mitigation mechanism [197]
	Man-in-the-middle	Multi-factor authentication of device and server [198]
	Unauthorized access	Attribute-based access control with HABACα [199]
	Routing and forwarding attacks	Trust-based computing with SCOTRES [200]
	Traffic analysis	IDS/IPS [201]
Physical	Loss of power and environmental threats	N/A
	Cloning	Quantum key distribution [175]
	Jamming	ML with SVM classifiers [211], trust-based authentication with TRAS [212]

Table 4. *Summary of threats and examples of countermeasures per IoT layer.*

5.3 Best-Practices Guide for a Secure Smart Home

As i presend in my work Vardakis G. et. al. “Review of Smart-Home Security Using the Internet of Things” [213], setting up a smart-home device involves careful planning and execution to ensure seamless integration, optimal performance, and security. Here is a best-practices guide to help you set up your smart home devices effectively:

1. Plan Your Smart Home Layout

    1. Identify Needs: Determine what you want your smart-home devices to accomplish. This could range from enhancing security to improve energy-efficiency or simply adding convenience to your daily routines.

    2. Select Compatible Devices: Choose devices that are compatible with each other and can be easily integrated into a single ecosystem. Look for devices that support common standards or platforms (e.g., Apple HomeKit, Google Home, Amazon Alexa).

2. Secure Your Devices

    1. Update/Upgrade Regularly: Set a process to automatically or periodically seek for and install updates/upgrades. Both for firmware and application software.

    2. Disposal Policy: Set safe disposal strategies for all equipment, including secure deletion/destruction of data and even physical destruction of digital components and memories/storage.

3. Device's Security Controls: Set all potential defenses that are provided by the main manufacturer (e.g., pins, extra security code, networking safeguards, etc.).

4. Minimize Exposure: Restrict connectivity to the least open/public LANs and networks that are necessary. Minimize the exposure of the system. 5. Set User Privileges: Restrict the number of authorized users to the minimum required. For each user, restrict access rights to the least privileges required.

6. Security Software: Set anti-virus, anti-malware, host-firewall, and host-IDS where applicable.

7. Delete Unnecessary Elements: Remove services, applications, or other elements that are insecure or not in use by the current system (e.g., Telnet).

8. Avoid Outdated Equipment: Do not use outdated devices that are not supported by the vendor anymore.

9. Configure Before Deployment: Before incorporating a new device to your system, verify that it is updated/upgraded, and all security and configurations are properly set.

3. Secure Applications and Software

1. Use Only Secure Versions: Install the latest secure and stable versions.

2. Set And Update Before Use: Upon installation, proceed immediately with the proper updates/upgrades, configurations, and settings of security/privacy.

3. Automate Updates: Set automated or periodic updates/upgrades.

4. Strong Authentication: Use strong passwords, as well as multi-factor authentication, wherever possible.

5. Application-Level Protections: Enable application-level firewalls, IDS, extra pins, or other defenses, wherever possible.

6. Restrict Access: Restrict access rights/permissions and connectivity to the minimum required.

7. Restrict Users: If applicable, restrict the number of users to the minimum required.

8. Use Official and Well-Reputed Vendors: Use only official and authenticated applications/software.

1. Especially for the technicians/engineers, always check the validity of the elements that are about to be installed (e.g., check the digital certification of the website, as well as the digest of the downloaded software).

2. For elements of unknown or less popular vendors, also check for recommendations from other users in related forums.

3. Do not install less trusted applications/software in the core of the system, especially if you have not tested them in a less critical part of your setting.

9. Monitor Operation: Where applicable, install security software for monitoring of the runtime environment and alerting.

10. Set Build-In Security and Privacy Controls: Check the offered options and set the privacy policies to the minimum required.

11. Secure Deletion: Apply secure removal strategies, logging out from all accounts and applications, revoking all acquired accesses/permissions, and securely erasing all permanent and temporary data.

12. Respond to Incidents: Set a response strategy, including details of whom you have to call and your first actions in case you notice something strange. For example, if you start receiving unknown notifications of purchase attempts in your mobile banking, you block your cards immediately and call your bank's 24/7 security service.

13. Recover from Incidents: Set a recovery strategy in case something happens.

4. Secure All Networks' Networking Devices

1. Security Configuration: Set the highest possible protections and set as a high priority the protection of the equipment that facilitates networking, especially for the devices that have direct access/exposure to Internet, and especially the main router.

2. Security Primitives: Activate or set additional firewalls and IDS/IPS. Use the most restrict policies possible.

3. Usage Zones: Create different LANs and virtual LANs (VLANs) for different usage zones of the smart home.

4. Remote Access: Consider setting an in-house virtual private network (VPN) for accessing the smart home remotely (e.g., the surveillance system).

5. Least Privileges: Restrict the privileges of services that are exposed to the Internet.

6. Network Monitoring: Install monitoring systems and periodically audit the activity of your system.

7. Decrease Attack Surface: Disable insecure communication protocols and services (e.g., http), as well as elements that are not currently in use.

8. Regular Updates: Similar with the devices, do not use outdated equipment.

5. Pay Specific Attention to Securing your Wi-Fi Network

1. Strong Passwords: Use strong, unique passwords for yourWi-Fi network and each of your smart-home devices.

2. Network Segmentation: Consider creating a separate Wi-Fi network for your smart devices to isolate them from the network you use for personal computing, reducing the risk of cross-device hacking.

3. Regular Updates: Keep your router's firmware and your smart devices' software up to date to protect against known vulnerabilities.

6. Install and Position your Devices Strategically

1. Follow Installation Guides: Carefully read and follow the installation instructions provided with your devices. This may include downloading an application, connecting to Wi-Fi, or performing initial setup steps.

2. Optimal Placement: Place devices in locations where they can function effectively (e.g., smart cameras with a clear field of view, smart thermostats away from direct sunlight).

7. Integrate Devices with a Central Hub or Application

1. Choose a Central Control System: Select a central hub or application that can control all your devices. This unifies control and makes managing your devices more convenient.

2. Customize Settings: Adjust settings for each device according to your preferences. This may involve setting schedules, creating automation rules, or defining scenes.

8. Test and Troubleshoot

1. Test Operations: After setting up, test your devices individually and the system as a whole to ensure they work as expected.

2. Troubleshoot Issues: If a device is not working correctly, consult the troubleshooting section of the device manual or contact customer support.

9. Educate Household Members

1. User Training: Educate all household members on how to use the smart devices, emphasizing the importance of security practices, like not sharing passwords.

2. Manage Your Passwords and Accounts: Consider utilizing password/

account managers.

3. Backup Your Data: Set a backup strategy.

10. Monitor and Adjust

1. Regular Reviews: Regularly review your smart-home setup to ensure it continues to meet your needs. Adjust settings, add new devices, or remove unnecessary ones as needed.

By following these best practices, you can create a smart-home setup that enhances convenience, efficiency, and security, while also being prepared to adapt to new technologies and needs over time.

5.4 Directions for Future Research

As smart-home environments become increasingly complex and interconnected—ranging from smart locks and surveillance cameras to lighting systems and voice-controlled assistants—the need for robust, adaptive, and privacy-preserving security mechanisms grows more urgent. Based on the synthesis of current challenges and technologies, the following unified list highlights key research and development areas for advancing smart-home security:

Key Research Topics and Innovation Areas

1. Enhanced Biometric Security

Development of advanced biometric methods leveraging device-specific capabilities (e.g., behavioral biometrics, facial recognition under varying lighting conditions).

2. Context-Aware Security Protocols

Adaptive protocols that dynamically respond to user location, behavior, and time-of-use to improve authentication and access control.

3. Decentralized Security Mechanisms

Application of blockchain and distributed ledger technologies to enhance identity management, access control, and data integrity.

4. Privacy-Enhancing Techniques

Advanced anonymization, local data processing, and federated learning approaches to minimize privacy risks in data collection.

5. Secure Multi-User Interactions

Mechanisms to manage access and privacy in shared device environments (e.g., smart TVs, AR/VR gear, shared IoT hubs).

6. Robust Malware Detection

Deployment of intelligent detection systems using behavioral analysis and AI to prevent malware in resource-constrained devices.

7. Physical and Network Security Integration

Holistic designs that merge physical hardware security (e.g., tamper detection) with secure communications and protocols.

8. Energy-Efficient Security Protocols

Development of lightweight encryption and security mechanisms for low-power devices (e.g., smart sensors, plugs).

9. Secure Device Management and Disposal

Full lifecycle management protocols to ensure security from deployment to decommissioning, including secure factory reset and data wiping.

10. International Security Standards for IoT

Promotion and development of universal security standards to unify protections across manufacturers and regions.

11. Anomaly Detection Using AI

Use of AI/ML to identify behavioral deviations, detect intrusions, and automate response in real-time.

12. IoT Device Interoperability and Security

Ensuring secure integration across diverse manufacturers and communication protocols, with standardized security baselines.

13. Ethical Design and User Consent

Incorporation of privacy-by-design and transparency to respect user autonomy and avoid hidden data collection.

14. Forensic Capabilities for IoT Security

Tools and methodologies for investigating incidents, collecting evidence, and reconstructing attack paths in smart-home environments.

15. Consumer Awareness and Education

Empowering users through education on best practices, risks, and privacy settings to enhance the human layer of security.

16. Regulatory Compliance and Privacy Laws

Ensuring adherence to local and international regulations (e.g., GDPR, CCPA), especially for cross-border IoT data flows.

17. Advanced Encryption Methods

Research into post-quantum cryptography, homomorphic encryption, and novel key exchange techniques for device-to-cloud and inter-device communication.

18. Hybrid Energy-Efficient Privacy-Preserving Schemes

Solutions balancing low energy consumption with strong privacy protection, suitable for bandwidth- and battery-limited environments.

This unified list addresses the multifaceted security and privacy challenges that smart-home environments face today. It reflects not only the technical necessities—like malware detection, secure device interactions, and anomaly response—but also broader social, ethical, and regulatory dimensions, including user consent, forensic readiness, and compliance with privacy laws.

As smart-home technologies become further embedded into everyday life, so too does the potential for unauthorized access, data interception, and network exploitation. These risks underscore the need for continuous innovation across device, network, and user layers. The future of smart-home security must embrace:

- Technological advancement (e.g., decentralized architectures, context-aware AI).
- Policy harmonization (e.g., global IoT security standards)
- User empowerment (e.g., awareness campaigns and intuitive security interfaces)

This thesis provides a roadmap for future research and development, promoting smarter, safer, and more user-respecting smart-home environments. By aligning innovation with user trust and regulatory foresight, we can create an IoT landscape that secures not just data, but also the everyday experiences of millions of users worldwide.

CHAPTER 6

Conclusions

In this thesis, I presented the technological foundations and methods that have been developed to enable the creation and advancement of smart homes. Special emphasis was placed on machine learning techniques—most notably, the Back Propagation algorithm for neural networks—used in applications such as face and silhouette recognition. While the primary focus was on their role in home security, the broader contributions of machine learning across domains, including medicine, were also acknowledged.

Modern security systems are increasingly reliant on facial recognition technologies to enhance protection, personalize user experiences, and streamline access within smart environments. Leading technology companies such as Netatmo, Netgear, Honeywell, and Ooma have integrated face recognition into their home security products to identify individuals approaching a property and detect potential intruders when the home is unoccupied. Honeywell, for example, has partnered with Amazon Alexa to develop a comprehensive home security solution that extends beyond traditional protection to encompass a fully smart-living experience. Similarly, Google's Nest Cam IQ provides 24/7 property surveillance with the capability to recognize individuals from distances up to 50 meters. These systems not only detect familiar faces but also allow users to define automated actions for specific individuals, such as unlocking doors or gates.

While facial recognition is rapidly transforming home security, it is also reshaping the technological and ethical landscape in which such systems are developed. The evolution of these technologies has highlighted the critical need for security—not only within the systems themselves but also in how they interact with and impact daily life.

To further improve the identification and mitigation of risks in smart homes, the adoption of formal modeling techniques—such as categorical logic—offers promising potential. This approach can be used to develop a comprehensive knowledge base, capable of executing queries in real time through IoT systems, creating intelligent interfaces that proactively detect and respond to potential threats [231,232].

As smart homes become increasingly interconnected through the proliferation of IoT devices, they also become more vulnerable to a range of cyber and physical threats. These include unauthorized access, data interception, and the exploitation of network vulnerabilities—each of which poses serious implications for user safety and privacy. The findings of this thesis reinforce the need for advanced security mechanisms, including enhanced biometric authentication, decentralized identity verification, advanced encryption, and AI-driven anomaly detection systems.

Equally important are the human-centric aspects of smart-home security. Consumer awareness, education, and responsible device management (including secure disposal) are vital components of a holistic security strategy. Future research must address these social and technical dimensions by developing privacy-enhancing technologies,

secure mechanisms for multi-user environments, and integrating physical safeguards with network-level protections.

Furthermore, the establishment of international standards and the exploration of decentralized technologies—such as blockchain—will be critical to harmonizing global security practices and strengthening resilience against evolving threats.

In conclusion, ensuring the security and privacy of smart-home environments is a multidimensional challenge that must keep pace with technological innovation. This thesis lays the groundwork for continued research and development aimed at fostering safer, smarter, and more secure living spaces. Through a combination of advanced technical solutions, regulatory alignment, and user-centric design, we can achieve a future where smart-home technologies are seamlessly integrated into everyday life—without compromising privacy, trust, or safety.

Bibliography

1. Xiao, G.; Guo, J.; Xu, L.D.; Gong, Z. User interoperability with heterogeneous IoT devices through transformation. IEEE Trans. Ind. Inform. 2014, 10, 1486–1496.

2. Chettri, L.; Bera, R. A Comprehensive Survey on Internet of Things (IoT) Toward 5GWireless Systems. IEEE Internet Things J. 2020, 7, 16–32.

3. Viani, F.; Robol, F.; Polo, A.; Rocca, P.; Oliveri, G.; Massa, A. Wireless architectures for heterogeneous sensing smart home applications: Concepts and real implementation. Proc. IEEE 2013, 101, 2381–2396.

4. Ndaguba, E.; Cilliers, J.; Ghosh, S.; Herath, S.; Mussi, E.T. Operability of Smart Spaces in Urban Environments: A Systematic Review on Enhancing Functionality and User Experience. Sensors 2023, 23, 6938.

5. Itair, M.; Shahrour, I.; Hijazi, I. The Use of the Smart Technology for Creating an Inclusive Urban Public Space. Smart Cities 2023, 6, 2484–2498.

6. Rani, S.; Chauhan, M.; Kataria, A.; Khang, A. IoT equipped intelligent distributed framework for smart healthcare systems. In Towards the Integration of IoT, Cloud and Big Data; Springer: Singapore, 2023; Volume 137, pp. 97–114.

7. Kapucu, N.; Bilim, M. Internet of Things for smart homes and smart cities. In Smart Grid 3.0; Springer: Cham, Germany, 2023; pp. 331–356.

8. Umair, M.; Cheema, M.A.; Afzal, B.; Shah, G. Energy management of smart homes over fog-based IoT architecture. Sustain. Comput. Inform. Syst. 2023, 39, 100898.

9. Padmanaban, S.; Nasab, M.A.; Shiri, M.E.; Javadi, H.H.S.; Nasab, M.A.; Zand, M.; Samavat, T. The role of Internet of Things in smart homes. In Artificial Intelligence-Based Smart Power Systems; Wiley: Hoboken, NJ, USA, 2022; Chapter 13.

10. Evans, D. The internet of things: How the next evolution of the internet is changing everything. Cisco Int. J. Internet 2011, 3, 123–132.

11. Fahrurozi, M.; Tarigan, S.A.; Alam Tanjung, M.; Mutijarsa, K. The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). In Proceedings of the 2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, Indonesia, 6–8 October 2020.

12. Ahmed, F.; Ko, Y. Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks. Secur. Commun. Netw. 2016, 9, 5143–5154.

13. Rawlinson, K. HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack; HP Advisory: Singapore, 2014.

14. Akram, H.; Konstantas, D.; Mahyoub, M. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 355–373.

15. Ahemd, M.M.; Shah, M.A.; Wahid, A. IoT security: A layered approach for attacks & defenses. In Proceedings of the 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, 19–21 April 2017; pp. 104–110.

16. Ahlawat, B.; Sangwan, A.; Sindhu, V. IoT system model challenges and threats. Int. J. Sci. Technol. Res. 2020, 9, 6771–6776. 14. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based smart home: Security challenges, security requirements and solutions. In Proceedings

of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017; pp. 1–6.

17. Gupta, B.B.; G Arachchilage, N.A.; Psannis, K.E. Defending against phishing attacks: Taxonomy of methods, current issues and future directions. Telecommun. Syst. 2018, 67, 247–267.

18. Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; Spanoudakis, G.; Frati, F.; Goeke, L.; Hildebrandt, T.; Tsakirakis, G.; Oikonomou, F.; Leftheriotis, G.; et al. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. Appl. Sci. 2020, 10, 5702.

19. Smyrlis, M.; Somarakis, I.; Spanoudakis, G.; Hatzivasilis, G.; Ioannidis, S. CYRA: A Model-Driven Cyber Range Assurance Platform. Appl. Sci. 2021, 11, 5165.

20. Zhu, P.; Hu, J.; Li, X.; Zhu, Q. Using Blockchain Technology to Enhance the Traceability of Original Achievements. IEEE Trans. Eng. Manag. 2023, 70, 1693–1707.

21. Touqeer, H.; Zaman, S.; Amin, R.; Hussain, M.; Al-Turjman, F.; Bilal, M. Smart home security: Challenges, issues and solutions at different IoT layers. J. Supercomput. 2021, 77, 14053–14089.

22. Almusaylim, Z.A.; Zaman, N. A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT). Wirel. Netw. 2019, 25, 3193–3204.

23. Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–175.

24. Gavra, V.D.; Dobra, I.M.; Pop, O.A. A survey on threats and security solutions for IoT. In Proceedings of the 2020 43rd International Spring Seminar on Electronics Technology (ISSE), Demanovska Valley, Slovakia, 14–15 May 2020; pp. 1–5.

25. Geneiatakis, D.; Kounelis, I.; Neisse, R.; Nai-Fovino, I.; Steri, G.; Baldini, G. Security and privacy issues for an IoT based smart home. In Proceedings of the 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 22–26 May 2017; pp. 1292–1297.

26. Kamrul, I.; Shen, W.; Wang, X. Security and privacy considerations for wireless sensor networks in smart home environments. In Proceedings of the 2012 IEEE 16th International Conference on Computer Supported CooperativeWork in Design (CSCWD), Wuhan, China, 23–25 May 2012; pp. 626–633.

27. Uand, J.; Sun, L. A Comprehensive Survey of Security Issues of Smart Home System: “Spear” and “Shields,” Theory and Practice. IEEE Access 2022, 10, 67–192.

28. Dahmen, J.; Cook, D.J.;Wang, X.; Honglei,W. Smart Secure Homes: A Survey of Smart Home Technologies that Sense, Assess, and Respond to Security Threats. J. Reliab. Intell. Environ. 2017, 3, 83–98.

29. Bastos, D.; Shackleton, M.; El-Moussa, F. Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28–29 March 2018.

30. Gendreau, A.A.; Moorman, M. Survey of intrusion detection systems towards an end to end secure internet of things. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 84–90.

31. Faisal, E.M.; Awad, A.I.; Hamed, H.F.A. Intrusion detection systems for IoT-based smart environments: A survey. J. Cloud Comput. 2018, 7, 1–20.

32. Datta, P.; Sharma, B. A survey on IoT architectures, protocols, security and smart city based applications. In Proceedings of the 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, 3–5 July 2017; pp. 1–5.

33. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smarthome IoT devices. In Proceedings of the 2015 IEEE 11th International Conference onWireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 19–21 October 2015; pp.1–5.

34. Isam, W.; Thomson, C.; Ghaleb, B. An RPL based optimal sensors placement in pipeline monitoring WSNs. In International Conference on Emerging Technologies and Intelligent Systems; Springer: Cham, Switzerland, 2021.

35. Li, H.; Chen, Y.; He, Z. The survey of RFID attacks and defenses. In Proceedings of the 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, China, 21–23 September 2012.

36. Yoon, S.; Park, H.; Yoo, H.S. Security issues on smarthome in IoT environment. In Computer Science and Its Applications; Springer: Berlin/Heidelberg, Germany, 2015; pp. 691–696.

37. Fariha, K.; Gawade, A. Secure Data Management in Smart Meter as an Application of IoT. Int. J. Sci. Res. (IJSR) 2016, 5, 1335–1337.

38. Kim, J.T.S. Analyses of Open Security Issues for Smart Home and Sensor Network Based on Internet of Things. IoT Appl. Comput. 2022, 11, 179–196.

39. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Netw. 2003, 1, 293–315.

40. Gill, R.K.; Sachdeva, M. Detection of hello flood attack on LEACH in wireless sensor networks. In Next-Generation Networks; Springer: Singapore, 2018; pp. 377–387.

41. Arabo, A.; Pranggono, B. Mobile malware and smart device security: Trends, challenges and solutions. In Proceedings of the 2013 19th International Conference on Control Systems and Computer Science, Bucharest, Romania, 29–31 May 2013; pp. 1–6.

42. Zhu, P.; Zhang, H.; Shi, Y.; Xie,W.; Pang, M.; Shi, Y. A novel discrete conformable fractional grey system model for forecasting carbon dioxide emissions. In Environment, Development and Sustainability; Springer: Berlin/Heidelberg, Germany, 2024; pp. 1–29.

43. Xu, X.; Chen, J.; Zhang, L.; Zhang, Z. Investigating smart home assistant security: A systematic literature review. IEEE Access 2020, 8, 186500–186512.

44. Santani, A.; Gangaramani, M.; Chopra, B.; Choudhary, P.; Samdani, K. An overview of architecture and security issues of a smart TV. In Proceedings of the 6th International Conference on Communication and Electronics Systems (ICCES-2021), Coimbatre, India, 8–10 July 2021; pp. 1835–1843.

45. De Guzman, J.A.; Thilakarathna, K.; Seneviratne, A. Security and Privacy Approaches in Mixed Reality: A Literature Survey. ACM Comput. Surv. 2019, 52, 1–37.

46. Dol, M.; Geetha, A. A Learning Transition from Machine Learning to Deep Learning: A Survey. In Proceedings of the 2021 International Conference on Emerging Techniques in Computational Intelligence (ICETCI), Hyderabad, India, 25–27 August 2021; pp. 89–94.

47. Chollet, F. Deep Learning with Python; Simon and Schuster: New York, NY, USA, 2021.

48. Liu, L.; Ouyang, W.; Wang, X.; Fieguth, P.; Chen, J.; Liu, X.; Pietikäinen, M. Deep learning for generic object detection: A survey. Int. J. Comput. Vis. 2020, 128, 261–318. [CrossRef]

49. LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning. Nature 2015, 521, 436–444. [CrossRef]

50. Ngiam, J.; Khosla, A.; Kim, M.; Nam, J.; Lee, H.; Ng, A.Y. Multimodal deep learning. In Proceedings of the 28th International Conference on Machine Learning, ICML 2011, Bellevue, WA, USA, 28 June–2 July 2011.

51. Kim, K.G. Deep Learning. Healthc Inform. Res. 2016, 22, 1075818. [CrossRef]

52. Këpuska, V.; Bohouta, G. Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home). In Proceedings of the 2018 IEEE 8th Annual Computing and CommunicationWorkshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 99–103.

53. Strickland, E. IBM Watson, heal thyself: How IBM overpromised and underdelivered on AI health care. IEEE Spectr. 2019, 56, 24–31.

54. Bini, S.A. Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: What do these terms mean and how will they impact health care? J. Arthroplast. 2018, 33, 2358–2361.

55. Van Ginneken, B. Fifty years of computer analysis in chest imaging: Rule-based, machine learning, deep learning. Radiol. Phys. Technol. 2017, 10, 23–32.

56. Ravi, D.; Wong, C.; Deligianni, F.; Berthelot, M.; Andreu-Perez, J.; Lo, B.; Yang, G.-Z. Deep learning for health informatics. IEEE J. Biomed. Health Inform. 2017, 21, 4–21.

57. Lillicrap, T. P., Santoro, A., Marris, L., Akerman, C. J., & Hinton, G. (2020). Backpropagation and the brain. *Nature Reviews Neuroscience*, *21*(6), 335-346.

58. Koenker, R. W., & d'Orey, V. (1987). Algorithm AS 229: Computing regression quantiles. *Applied statistics*, 383-393.

59. Vardakis, G., Tsamis, G., Koutsaki, E., Haridimos, K., & Papadakis, N. (2022). Smart home: Deep learning as a method for machine learning in recognition of face, silhouette and human activity in the service of a safe home. Electronics, 11(10), 1622.

60. Hahnloser, R. L. (1998). On the piecewise analysis of networks of linear threshold neurons. *Neural Networks*, *11*(4), 691-697.

61. Ostojic, S., & Brunel, N. (2011). From spiking neuron models to linear-nonlinear models. *PLoS computational biology*, *7*(1), e1001056.

62. Carson, Y., & Maria, A. (1997, December). Simulation optimization: methods and applications. In *Proceedings of the 29th conference on Winter simulation* (pp. 118-126).

63. Arshad, M. H., Bilal, M., & Gani, A. (2022). Human activity recognition: Review, taxonomy and open challenges. *Sensors*, *22*(17), 6463.

64. Robert Hecht-Nielsen HNC Inc.; University of California San Diego. Theory of the Backpropagation Neural Network. In Neural Networks for Perception; Elsevier: Amsterdam, The Netherlands, 1992.

65. Zhang, J.; Zhang, J.; Lok, T.; Lyu, M.R. A hybrid particle swarm optimization–back-propagation algorithm for feedforward neural network training. Appl. Math. Comput. 2007, 185, 1026–1037.

66. Chen, F.-C. Back-Propagation Neural Networks for Nonlinear Self -Tuning Adaptive Control. IEEE Control Syst. Mag. 1990, 10, 44–48.

67. Jalal, A.; Kamal, S.; Hee, K. Real-Time life logging via a depth silhouette-based human activity recognition system for smart home services. In Proceedings of the 2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Seoul, Korea, 26–29 August 2014.

68. Chen, S.; Ding, S.; Fu, H.; Xian, Y.; Liu, X.; Zhang, C. Deep learning applied to smart home face recognition access control system. In Proceedings of the 2018 2nd International Conference on Artificial Intelligence: Technologies and Applications (ICAITA 2018), Hong Kong, 25–26 March 2018.

69. Sutskever, I.; Martens, J.; Dahl, G.; Hinton, G. On the importance of initialization and momentum in deep learning. In Proceedings of the 30th International Conference on Machine Learning, Atlanta, GA, USA, 16–21 June 2013; Volume 28, pp. 1139–1147.

70. Pawar, S.; Kithani, V.; Ahuja, S.; Sahu, S. Smart home security using IoT and face recognition. In Proceedings of the 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16–18 August 2018.

71. Ratna, D.A.; Abadianto,W.D. Design of face detection and recognition system for smart home security application. In Proceedings of the 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 1–2 November 2017.

72. Meera, M.; Divya, R.S. Super secure door lock system for critical zones. In Proceedings of the 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvananthapuram, India, 20–22 July 2017.

73. Anwar, S.; Kishore, D. IOT based smart home security system with alert and door access control using smart phone. Int. J. Eng. Res. Technol. IJERT 2016, 5, 504–509.

74. Zuo, F.; Peter, H.; de With, N. Real-time Embedded Face Recognition for Smart Home. IEEE Trans. Consum. Electron. 2005, 51, 183–190.

75. Yi, S.; Hao, Z.; Qin, Z.; Li, Q. Fog computing: Platform and applications. In Proceedings of the 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb),Washington, DC, USA, 12–13 November 2015.

76. Patsadu, O.; Nukoolkit, C.;Watanapa, B. Human Gesture Recognition Using Kinect Camera. In Proceedings of the 2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE), Bangkok, Thailand, 30 May–1 June 2012.

77. Abdi, N.; Ramokapane, K.M.; Such, J.M. More than smart speakers: Security and privacy perceptions of smart home personal assistants. In Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS 2019), USENIX Association, Santa Clara, CA, USA, 11–13 August 2019; pp. 451–466.

78. Zhang, L.; Wang, X.; Tan, Z.; Chen, J.; Xu, X.; Zhang, Z. Voice hacking: Evaluating voice-controlled smart home assistant's vulnerability against replay attacks. IEEE Internet Things J. 2021, 8, 7319–7330.

79. Zhang, Z.; Chen, J. Voice assistant security: A review of attack scenarios and defenses. IEEE Secur. Priv. 2019, 17, 22–29.

80. Xiao, Y.; Jiang, C.; Huang, D.; Liang, K. Secure and efficient access control for smart home assistant. J. Ambient. Intell. Humaniz. Comput. 2021, 12, 4545–4554.

81. Obaid, A. Assessment of Smart Home Assistants as an IoT. Int. J. Comput. Inf. Manuf. (IJCIM) 2021, 1, 18–36. [CrossRef]

82. Alam, I.; Khusro, S.; Naeem, M. A review of smart TV: Past, present, and future. In Proceedings of the International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 5 February 2018; pp. 35–41.

83. Bachy, Y.; Basse, F.; Nicomette, V.; Alata, E.; Kaaniche, M.; Courrege, J.; Lukjanenko, P. Smart-TV security analysis: Practical experiments. In Proceedings of the 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Rio de Janeiro, Brazil, 22–25 June 2015; pp. 497–504.

84. Bao, L.; Wu, S.; Yu, S.; Huang, J. Client-side Security Assessment and Security Protection Scheme for Smart TV Network. In Proceedings of the 6th International Conference on Computer and Communications, Chengdu, China, 11–14 December 2020; Pp . 573–578.

85. Zhang, Y.; Ma, S.; Chen, T.; Li, J.; Deng, R.H.; Bertino, E. EvilScreen Attack: Smart TV Hijacking via Multi-channel Remote Control Mimicry. IEEE Trans. Dependable Secur. Comput. 2023, 21, 1544–1556.

86. Claverie, T.; Lopes Esteves, J.; Kasmi, C. Smart TVs: Security of DVB-T. In Proceedings of the Information and Communications Technology Security Symposium (SSTIC), Rennes, France, 14 June 2018; pp. 73–106.

87. Aluri, D.C. Smart lock systems: An overview. Int. J. Comput. Appl. 2020, 177, 40–43.

88. Kalbo, N.; Mirsky, Y.; Shabtai, A.; Elovici, Y. The security of IP-Based video surveillance systems. Sensors 2020, 20, 4806.

89. Nguyen, T. A deep look into privacy and security of vacuum robot. In Proceedings of the 20th Annual Cybersecurity & Awareness Fair (CyberFair), Pomona, CA, USA, 17 October 2024; pp. 1–7.

90. Ronen, E.; Shamir, A. Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. In Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), Saarbruecken, Germany, 21–24 March 2016; pp. 1–10.

91. Huchuk, B.; Sanner, S.; O'Brien, W. Development and evaluation of data-driven controls for residential smart thermostats. Energy Build. 2021, 249, 111201.

92. Hariadi, R.R.; Yuniarti, A.; Kuswardayan, I.; Herumurti, D.; Arifiani, S.; Yunanto, A.A. Termo: Smart air conditioner controller integrated with temperature and humidity sensor. In Proceedings of the 12th International Conference on Information & Communication Technology and System (ICTS), Surabaya, Indonesia, 18 July 2019; pp. 1–6.

93. Reid, S.E.; Abdulrazak, B.; Alas, M. Proof of Concept Evaluation for an Intelligent Oven. Enhanc. Qual. Life Smart Living 2017, 10461, 161–172.

94. Nasir, H.; Aziz, W.B.W.; Ali, F.; Kadir, K.; Khan, S. The Implementation of IoT based Smart Refrigerator System. In Proceedings of the 2nd International Conference on Smart Sensors and Application (ICSSA), Kuching, Malaysia, 24–26 July 2018; pp. 48–52.

95. Gomes, L.; Sousa, F.; Vale, Z. An Intelligent Smart Plug with Shared Knowledge Capabilities. Sensors 2018, 18, 3961.

96. Horák, T.; Huraj, L. Smart Thermostat as a Part of IoT Attack. In Proceedings of the 8th Computer Science On-line Conference, Cybernetics and Automation Control Theory Methods in Intelligent Algorithms (AISC), Zlin, Czech Republic, 24–27 April 2019; Volume 3, pp. 156–163.

97. Wang, A.; Nirjon, S. A False Sense of Home Security—Exposing the Vulnerability in Away Mode of Smart Plugs. In Proceedings of the IEEE International Conference on Pervasive Computing and CommunicationsWorkshops (PerComWorkshops), Kyoto, Japan, 11–15 March 2019; pp. 316–321.

98. Liu, P.; Ji, S.; Fu, L.; Lu, K.; Zhang, X.; Qin, J.; Wang,W.; Chen,W. How IoT re-using threatens your sensitive data: Exploring the User-Data disposal in used IoT devices. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–25 May 2023; pp. 1–17.

99. Shuhaiber, A.; Ahim Mashal, I. Understanding users' acceptance of smart homes. Technol. Soc. 2010, 58, 1011109.

100. Këpuska, V.; Bohouta, G. Next-generation of virtual personal assistants (Microsoft Cortana, Apple Siri, Amazon Alexa and Google Home). In Proceedings of the IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2018; pp. 1–8.

101. Fruchter, N.; Liccardi, I. Consumer Attitudes Towards Privacy and Security in Home Assistants. In Proceedings of the CHI Conference on Human Factors in Computing Systems, New York, NY, USA, 21–26 April 2018; Article LBW050. pp. 1–6.

102. Lei, X.; Tu, G.; Liu, A.X.; Li, C.; Xie, T. The Insecurity of Home Digital Voice Assistants-Vulnerabilities, Attacks and Countermeasures. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–9.

103. Sudharsan, B.; Corcoran, P.; Ali, M.I. Smart speaker design and implementation with biometric authentication and advanced voice interaction capability. In Proceedings of the AIAI Irish Conference on Artificial Intelligence and Cognitive Science, Galway, Ireland, 5–6 December 2019; pp. 1–14.

104. Corbett, C.F.; Combs, E.M.; Wright, P.J.; Owens, O.L.; Stringfellow, I.; Nguyen, T.; Van Son, C.R. Virtual Home Assistant Use and Perceptions of Usefulness by Older Adults and Support Person Dyads. Int. J. Environ. Res. Public Health 2021, 18, 1113.

105. Diogo Vieira, A.; Leite, H.; Vitória Lachowski Volochtchu, A.K. The impact of voice assistant home devices on people with disabilities: A longitudinal study. Technol. Forecast. Soc. Change 2022, 184, 121961.

106. Triyono, L.; Yudantoro, T.R.; Sukamto, S.; Hestinigsih, I. VeRO: Smart home assistant for blind with voice recognition. Mater. Sci. Eng. 2021, 1108, 012016.

107. Beirl, D.; Rogers, Y.; Yuill, N. "Using Voice Assistant Skills in Family Life. In Proceedings of the International Conference on Computer Supported Collaborative Learning—A Wide Lens: Combining Embodied, Enactive, Extended, and Embedded Learning in Collaborative Settings (CSCL), Lyon, France, 17–21 June 2019; pp. 1–8.

108. Zhu, P.; Miao, C.; Wang, Z.; Li, X. Informational cascade, regulatory focus and purchase intention in online flash shopping. Electron. Commer. Res. Appl. 2023, 62, 16474–16496.

109. Edu, J.S.; Such, J.M.; Suarez-Tangil, G. Smart home personal assistants: A security and privacy review. ACM Comput. Surv. 2019, 53, 116.

110. Qamar, S.; Anwar, Z.; Afzal, M. A systematic threat analysis and defense strategies for the metaverse and extended reality systems. Comput. Secur. 2023, 128, 103127.

111. Duezguen, R.; Mayer, P.; Das, S.; Volkamer, M. Towards Secure and Usable Authentication for Augmented and Virtual Reality Head-Mounted Displays. In Proceedings of the Who Are You?! Adventures in Authentication (WAY), Virtual Event, 7 August 2020; pp. 1– 6.

112. Stephenson, S.; Pal, B.; Fan, S.; Fernandes, E.; Zhao, Y.; Chatterjee, R. SoK: Authentication in augmented and virtual reality. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 22–26 May 2022; pp. 267–284.

113. Ali, M.; Naeem, F.; Kaddoum, G.; Hossain, E. Metaverse communications, networking, security, and applications: Research issues, State-of-the-Art, and future directions. IEEE Commun. Surv. Tutor. 2024, 26, 1238–1278.

114. Buldeo Rai, H.; Verlinde, S.; Macharis, C. Unlocking the failed delivery problem? Opportunities and challenges for smart locks from a consumer perspective. Res. Transp. Econ. 2021, 87, 100753.

115. Ho, G.; Leung, D.; Mishra, P.; Hosseini, A.; Song, D.;Wagner, D. Smart Locks: Lessons for Securing Commodity Internet of Things Devices. In Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security (ASIA CCS), Xi'an, China, 30 May–3 June 2016; pp. 461–472.

116. De Camargo Silva, L.; Samaniego, M.; Deters, R. IoT and Blockchain for Smart Locks. In Proceedings of the 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 17–19 October 2019; pp. 262–269.

117. Nadiya, U.; Ilham Rizqyawan, M.; Mahnedra, O. Blockchain-based Secure Data Storage for Door Lock System. In Proceedings of the 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 20–21 November 2019; pp. 140–144.

118. Raizada, P.; Gupta, S.; Das, M.; Rastogi, P.; Arora, D. Smart Lock System using IoT, Embedded & Machine Learning. In Proceedings of the 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2022; pp. 1–8.

119. Hazazi, H.; Shehab, M. Exploring the Usability, Security, and Privacy of Smart Locks from the Perspective of the End User. In Proceedings of the 9th Symposium on Usable Privacy and Security, USENIX, Anaheim, CA, USA, 7–8 August 2023; pp. 559–577.

120. Pandya, S.; Ghayvat, H.; Kotecha, K.; Awais, M.; Akbarzadeh, S.; Gope, P.; Mukhopadhyay, S.C.; Chen, W. Smart home anti-theft system: A novel approach for near real-time monitoring and smart home security for wellness protocol. Appl. Syst. Innov. 2018, 1, 42.

121. Abdalla, P.A.; Varol, C. Testing IoT security: The case study of an IP camera. In Proceedings of the 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, Lebanon, 1–2 June 2020; pp. 1–5.

122. Tekeoglu, A.; Saman Tosun, A. Investigating security and privacy of a cloud-based wireless IP camera: NetCAM. In Proceedings of the 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas, NV, USA, 3–6 August 2015; pp. 1–6.

123. Stolojescu-Crisan, C.; Crisan, C.; Butunoi, B. Access control and surveillance in a smart home. High-Confid. Comput. 2022, 2, 1–9.

124. Wan, Y.; Xu, K.; Xue, G.; Wang, F. IoTArgos: A multi-layer security monitoring system for Internet-of-Things in smart homes. In Proceedings of the IEEE Conference on Computer Communications (INFOCOM), Toronto, ON, Canada, 6–9 July 2020; pp. 1–10.

125. Sami, S.; Dai, Y.; Tan, S.R.X.; Roy, N.; Han, J. Spying with your robot vacuum cleaner: Eavesdropping via lidar sensors. In Proceedings of the 18th ACM Conference on Embedded Networked Sensor Systems (SenSys'20), Virtual Event, Japan, 16–19 November 2020; pp. 1–14.

126. ISO/IEC 30141:2018; Internet of Things (IoT) Reference Architecture. 2018. Available online: https://www.iso.org/standard/6569 5.html (accessed on 19 February 2024).

127. Kim, S. IEEE 2413-2029; IEEE Standard for an Architectural Framework for the Internet of Things (IoT). IEEE Standards Association, 2019. Available online: https://standards.ieee.org/ieee/2413/6226/ (accessed on 19 February 2024).

128. Iiconsortium. The Industrial Internet Reference Architecture. Industry IoT Consortium. 2022. Available online: https://www. iiconsortium.org/iira/ (accessed on 19 February 2024).

129. OCF. OCF Specification 2.2.7. Open Connectivity Foundation, 2021. Available online: https://openconnectivity.org/developer/ specifications/ (accessed on 19 February 2024).

130. NIST. NIST Cybersecurity Framework 2.0. 2024. Available online: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurityframework- 20/ipd (accessed on 19 February 2024).

131. Vo, J. NIST SP 800-13–Network of Things. NIST, 2016. Available online: https://csrc.nist.gov/pubs/sp/800/183/final (accessed on 19 February 2024).

132. Wu, M.; Lu, T.J.; Ling, F.Y.; Sun, J.; Du, H.Y. Research on the architecture of Internet of Things. In Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Chengdu, China, 20–22 August 2010; pp. 484–487.

133. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. Futur. Gener. Comput. Syst. 2019, 100, 144–164.

134. Li, S.; Tryfonas, T.; Li, H. The internet of things: A security point of view. Internet Res. 2016, 26, 337–359.

135. Sethi, P.; Sarangi, S.R. Internet of things: Architectures, protocols, and applications. J. Electr. Comput. Eng. 2017, 2017, 1–25.

136. Suo, H.; Wan, J.; Zou, C.; Liu, J. Security in the internet of things: A review. In Proceedings of the 2012 International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012; Volume 3, p. 373.

137. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social engineering attack strategies and defence approaches. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 145–149.

138. He, D.; Ye, R.; Chan, S.; Guizani, M.; Xu, Y. Privacy in the internet of things for smart healthcare. IEEE Commun. Mag. 2018, 56, 38–44.

139. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. In Proceedings of the 7th International Conference on Body Area Networks (BODYNETS), Oslo, Norway, 24–26 September 2012; pp. 1–7.

140. Xu, X. Study on security problems and key technologies of the internet of things. In Proceedings of the 2013 International Conference on Computational and Information Sciences, Shiyang, China, 21–23 June 2013.

141. Nirmal, K.; Janet, B.; Kumar, R. Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection. Peer-to-Peer Netw. Appl. 2021, 14, 2327–2339.

142. Whittaker, C.; Ryner, B.; Nazif, M. Large-scale automatic classification of phishing pages. In Proceedings of the Network and Distributed System Security Symposium (Ndss), San Diego, CA, USA, 28 February–3 March 2010; pp. 1–14.

143. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.

144. Wei, D.; Qiu, X. Status-based detection of malicious code in Internet of Things (IoT) devices. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018; pp. 1–7.

145. Sharma, P.; Zawar, S.; Pati, S.B. Ransomware analysis: Internet of Things (Iot) security issues challenges and open problems in the context of worldwide scenario of security of systems and malware attacks. Manag. J. Innov. Res. Sci. Eng. (IJIRSE) 2016, 2, 177–184.

146. Stamelos, I.; Hatzivasilis, G.; Ioannidis, S. Active HoneyFiles for Ransomware Encryption Mitigation. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (IEEE CSR)Workshops, London, UK, 2–4 September 2024; pp. 1–8.

147. Cesare, S. Breaking the security of physical devices. In Proceedings of the Black Hat USA 2014, Las Vegas, NV, USA, 2–7 August 2014; pp. 1–7.

148. Hossain, M.M.; Fotouhi, M.; Hasan, R. Towards an analysis of security issues, challenges, and open problems in the internet of things. In Proceedings of the 2015 IEEEWorld Congress on Services, New York, NY, USA, 27 June–2 July 2015; pp. 21–28.

149. Varga, P.; Plosz, S.; Soos, G.; Hegedus, C. Security threats and issues in automation IoT. In Proceedings of the 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Trondheim, Norway, 31 May–2 June 2017; pp. 1–6.

150. Hassija, V.; Chamola, V.; Saxena, V.; Jain, D.; Goyal, P.; Sikdar, B. A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access 2019, 7, 82721–82743.

151. Zhao, W.; Yang, S.; Luo, X. On threat analysis of IoT-based systems: A survey. In Proceedings of the 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), Beijing, China, 14–16 August 2020; pp. 205–212.

152. Kim, D. Cyber security issues imposed on nuclear power plants. Ann. Nucl. Energy. 2014, 65, 141–143.

153. Denning, D.E. Stuxnet: What has changed? Future Internet 2012, 4, 672–687.

154. Ko, E.; Kim, T.; Kim, H. Management platform of threats information in IoT environment. J. Ambient. Intell. Humaniz. Comput. 2018, 9, 1167–1176.

155. Ganguly, P.; Nasipuri, M.; Dutta, S. A novel approach for detecting and mitigating the energy theft issues in the smart metering infrastructure. Technol. Econ. Smart Grids Sustain. Energy. 2018, 3, 1–11.

156. Alnaeli, S.M.; Sarnowski, M.; Aman, M.S.; Abdelgawad, A.; Yelamarthi, K. Vulnerable C/C++ code usage in IoT software systems. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016; pp. 348–352.

157. Werner, M.; Unterluggauer, T.; Schaffenrath, D.; Mangard, S. Sponge-based control-flow protection for IoT devices. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 214–226.

158. Mujica, G.; Portilla, J. Distributed reprogramming on the edge: A new collaborative code dissemination strategy for IoT. Electronics 2019, 8, 267.

159. Abbas, S.G.; Vaccari, I.; Hussain, F.; Zahid, S.; Fayyaz, U.U.; Shah, G.A.; Bakhshi, T.; Cambiaso, E. Identifying and Mitigating Phishing Attack Threats in IoT Use Cases Using a Threat Modelling Approach. Sensors 2021, 21, 4816.

160. Li, X.; Zhang, D.; Wu, B. Detection method of phishing email based on persuasion principle. In Proceedings of the IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020; pp. 571–574.

161. Nishikawa, H.; Yamamoto, T.; Harsham, B.; Wang, Y.; Uehara, K.; Hori, C.; Iwasaki, A.; Kawauchi, K.; Nishigaki, M. Analysis of Malicious Email Detection using Cialdini's Principles. In Proceedings of the 15th Asia Joint Conference on Information Security (AsiaJCIS), Taipei, Taiwan, 20–21 August 2020; pp. 137–142.

162. Sonowal, G. Phishing Email Detection Based on Binary Search Feature Selection. SN Comput. Sci. 2020, 1, 191.

163. Sahingoz, O.K.; Buber, E.; Demir, O.; Diri, B. Machine learning based phishing detection from URLs. Expert. Syst. Appl. 2019, 117, 345–357.

164. Ficco, M. Detecting IoT malware by Markov chain behavioral models. In Proceedings of the IEEE International Conference on Cloud En-gineering (IC2E), Prague, Czech Republic, 24–27 June 2019; pp. 229–234.

165. Sharmeen, S.; Huda, S.; Abawajy, J.H.; Ismail, W.N.; Hassan, M.M. Malware threats and detection for industrial Mobile-IoT networks. IEEE Access 2018, 6, 15941–15957.

166. Wang, W.; Zhao, M.; Gao, Z.; Xu, G.; Xian, H.; Li, Y.; Zhang, X. Constructing features for detecting android malicious applications: Issues, taxonomy and directions. IEEE Access 2019, 7, 67602–67631.

167. Nimmy, K.; Sankaran, S.; Achuthan, K. A novel multi-factor authentication protocol for smart home environments. In Information Systems Security (ICISS); Springer: Cham, Germany, 2018; Volume 11281, pp. 44–63.

168. Nimmy, K.; Sankaran, S.; Achuthan, K.; Calyam, P. Lightweight and privacy-preserving remote user authentication for smart homes. IEEE Access 2022, 10, 176–190.

169. Nagy, R.; Németh, K.; Papp, D.; Buttyán, L. Rootkit detection on embedded IoT devices. Acta Cybern. 2021, 25, 369–400.

170. Haney, J.M.; Furman, S.M. Smart Home Updates: User Perceptions and Experiences. In Proceedings of the Symposium on Security and Privacy (SP), San Francisco, CA, USA, 21–25 May 2023; pp. 1–5.

171. Haney, J.M.; Furman, S.M. Work in progress: Towards usable updates for smart home devices. In Proceedings of the Socio- Technical Aspects in Security and Trust (STAST),

Virtual Event, 14 September 2020; Springer: Cham, Switzerland, 2021; Volume 12812, pp. 107–117.

172. Classen, J.; Chen, J.; Steinmetzer, D.; Hollick, M.; Knightly, E. The spy next door: Eavesdropping on high throughput visible light communications. In Proceedings of the 2nd International Workshop on Visible Light Communications Systems, New York, NY, USA, 11 September 2015; pp. 9–14.

173. Kaur, M.; Kalra, S. Security in IoT-Based smart grid through quantum key distribution. Adv. Intell. Syst. Comput. 2018, 2, 523–530.

174. Fakhri, D.; Kusprasapta, M. Secure IoT communication using blockchain technology. In Proceedings of the 2018 international Symposzium on Electronics and Smart Devices (ISESD), Bandung, Indonesia, 23–24 October 2018; pp. 1–6.

175. Das, D.; Maity, S.; Nasir, S.B.; Ghosh, S.; Raychowdhury, A.; Sen, S. High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In Proceedings of the 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Mclean, VA, USA, 1–5 May 2017; pp. 62–67.

176. Siddiqui, S.T.; Alam, S.; Ahmad, R.; Shuaib, M. Security threats, attacks, and possible countermeasures in internet of things. Lect. Notes Netw. Syst. 2020, 35–46. [CrossRef]

177. Hariri, R.H.; Fredericks, E.M.; Bowers, K.M. Uncertainty in big data analytics: Survey, opportunities, and challenges. J. Big Data 2019, 6, 1–16.

178. Kanuparthi, A.; Karri, R.; Addepalli, S. Hardware and embedded security in the context of internet of things. In Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles, Berlin, Germany, 4 November 2013; pp. 61–64.

179. Abrishamchi, M.N.; Abdullah, A.H.; Cheok, A.D.; Nikolic, P.K. A probability based hybrid energy-efficient privacy preserving scheme to encounter with wireless traffic snooping in smart home. In Proceedings of the 2nd EAI International Summit, Smart City 360◦, Bratislava, Slovakia, 22–24 November 2017; pp. 1–10.

180. Zeng, X.; Martinez, T. A noise filtering method using neural networks. In Proceedings of the IEEE InternationalWorkshop on Soft Computing Techniques in Instrumentation, Measurement and Related Applications, Provo, UT, USA, 17 May 2003; pp. 26–31.

181. Li, Z.; Yin, X.; Geng, Z.; Zhang, H.; Li, P.; Sun, Y.; Zhang, H.; Li, L. Research on PKI-like Protocol for the Internet of Things. In Proceedings of the 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, Hong Kong, China, 16–17 January 2013; pp. 915–918.

182. Liu, Y.; Briones, J.; Zhou, R.; Magotra, N. Study of secure boot with a FPGA-based IoT device. In Proceedings of the 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), Boston, MA, USA, 6–9 August 2017; pp. 1053–1056.

183. Arı¸s, A.; Oktu˘ g, S.F.; Yalçın, S.B.Ö. Internet-of-Things security: Denial of service attacks. In Proceedings of the 2015 23rd Signal Processing and Communications Applications Conference (SIU), Malatya, Turkey, 16–19 May 2015; pp. 1–4.

184. Abhishek, N.V.; Tandon, A.; Lim, T.J.; Sikdar, B. Detecting forwarding misbehavior in clustered IoT networks. In Proceedings of the 14th ACM International Symposium on QoS and Security forWireless and Mobile Networks, Montrea, QC, Canada, 28 October–2 November 2018; pp. 1–6.

185. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of things: Evolution and technologies from a security perspective. Sustain. Cities Soc. 2020, 54, 101728.

186. Ashibani, Y.; Mahmoud, Q.H. A behavior profiling model for user authentication in IoT networks based on app usage patterns. In Proceedings of the IECON 2018—44th Annual Conference of the IEEE Industrial Electronics Society,Washington, DC, USA, 21–23 October 2018; pp. 2841–2846.

187. Hossain, M.; Riazul Islam, S.M.; Ali, F.; Kwak, K.; Hasan, R. An internet of things-based health prescription assistant and its security system design. Futur. Gener. Comput. Syst. 2018, 82, 422–439.

188. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. IEEE Commun. Surv. Tutor. 2020, 22, 1686–1721.

189. Arora, A.; Kaur, A.; Bhushan, B.; Saini, H. Security concerns and future trends of internet of things. In Proceedings of the 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Kannur, India, 5–6 July 2019; pp. 891–896.

190. Asif, W.; Ray, I.G.; Rajarajan, M. An attack tree based risk evaluation approach for the internet of things. In Proceedings of the 8th International Conference on the Internet of Things, Santa Barbara, CA, USA, 15–18 October 2018; pp. 1–8.

191. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized Privacy-Preserving healthcare blockchain for IoT. Sensors 2019, 19, 326.

192. Aziz, T.; Haq, E. Security challenges facing IoT layers and its protective measures. Int. J. Comput. Appl. 2018, 179, 31–35.

193. Kim, Y.; Yoo, S.; Yoo, C. DAoT: Dynamic and energy-aware authentication for smart home appliances in Internet of Things. In Proceedings of the 2015 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 9–12 January 2015; pp. 196–197.

194. Kamel, S.O.; Hegazi, N.H. A proposed model of IoT security management system based on a study of internet of things (IoT) security. Int. J. Sci. Eng. Res. 2018, 9, 1227–1244.

195. Hatzivasilis, G.; Soultatos, O.; Chatziadam, P.; Fysarakis, K.; Askoxylakis, I.; Ioannidis, S.; Alexandris, G.; Katos, V.; Spanoudakis, G. WARDOG: Awareness detection watchdog for botnet infection on the host device. IEEE Trans. Sustain. Comput. 2019, 4, 1–15.

196. Aliyu, F.; Sheltami, T.; Shakshuki, E.M. A detection and prevention technique for man in the middle attack in fog computing. Procedia Comput. Sci. 2018, 141, 24–31.

197. Ameer, S.; Benson, J.; Sandhu, R. An Attribute-Based Approach toward a Secured Smart-Home IoT Access Control and a Comparison with a Role-Based Approach. Information 2022, 13, 60.

198. Hatzivasilis, G.; Papaefstathiou, I.; Manifavas, C. SCOTRES: Secure Routing for IoT and CPS. IEEE Internet Things J. (IoT) 2017, 4, 2129–2141.

199. Rajora, C.S.; Sharma, A. IoT Based Smart Home with Cutting-Edge Technology for IDS/IPS. In Proceedings of the 2nd International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE), Bangalore, India, 16–17 December 2022; pp. 1–5.

200. Atlam, H.F.; Wills, G.B. IoT security, privacy, safety and ethics. In Digital Twin Technologies and Smart Cities; Springer: Cham, Switzerland, 2020; pp. 123–149.

201. Ida, I.B.; Jemai, A.; Loukil, A. A survey on security of IoT in the context of eHealth and clouds. In Proceedings of the 2016 11th International Design & Test Symposium (IDT), Hammamet, Tunisia, 18–20 December 2016; pp. 25–30.

202. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of Things: Security vulnerabilities and challenges. In Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus, 6–9 July 2015; pp. 180–187.

203. Meng, S.; Gao, Z.; Li, Q.; Wang, H.; Dai, H.N.; Qi, L. Security-Driven hybrid collaborative recommendation method for cloud-based iot services. Comput. Secur. 2020, 97, 101950.

204. Jayakumar, H.; Raha, A.; Kim, Y.; Sutar, S.; Lee, W.S.; Raghunathan, V. Energy-efficient system design for IoT devices. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macao, China, 25–28 January 2016; pp. 298–301.

205. Kalra, N.; Sharma, A.; Kumar, N.; Singh, R.; Gehlot, A. Design and development of IoT-based transmission line monitoring system. In Intelligent Communication, Control and Devices; Springer: Singapore, 2018; pp. 465–471.

206. Dou, Z.; Si, G.; Lin, Y.; Wang, M. An adaptive resource allocation model with anti-jamming in IoT network. IEEE Access 2019, 7, 93250–93258.

207. Choi, J.; Jin, S.I. Security threats in connected car environment and proposal of in-vehicle infotainment-based access control mechanism. In Advanced Multimedia and Ubiquitous Engineering; Springer: Singapore, 2018; pp. 383–388.

208. Rodrigues, L.; Guerreiro, J.; Correia, N. RELOAD/CoAP architecture for the federation of wireless sensor networks. Peer-to-Peer Netw. Appl. 2020, 13, 27–37.

209. Jeyaselvi, M.; Sathya, M.; Suchitra, S.; Jafar Ali Ibrahim, S.; Kalyan Chakravarthy, N.S. SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks. In Advances in Information Communication Technology and Computing; Springer: Singapore, 2022; Volume 392, pp. 461–471.

210. Mbarek, B.; Ge, M.; Pitner, T. Trust-Based Authentication for Smart Home Systems. In Wireless Personal Communications; Springer: Berlin/Heidelberg, Germany, 2021; Volume 117, pp. 2157–2172.

211. Sati, V.; Garg, D.; Choudhury, T.; Aggarwal, A. Facial Recognition-Application and Future: A Review. In Proceedings of the 2018 International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 23–24 November 2018; pp. 231–235.

212. Kim, K.; Lee, J.; Jung, W. Method of building a security vulnerability information collection and management system for analyzing the security vulnerabilities of IoT devices. In Advanced Multimedia and Ubiquitous Engineering; Springer: Singapore, 2017; Volume 448, pp. 205–210.

213. Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. Electronics, 13(16), 3343.

214. David, E.; Stolfo, S. Guest Editors Introduction: The Science of Security. IEEE Secur. Priv. 2011, 9, 16–17.

215. Nicol, D.M.; Sanders,W.H.; Scherlis,W.L.;Williams, L.A. Science of Security Hard Problems: A Lablet Perspective. Science of Security Virtual OrganizationWeb. 2012. Available online: https://cps-vo.org/node/6394 (accessed on 30 March 2022).

216. McGraw, G.; Migues, S.; West, J. Building Security in Maturity Model. 2017. Available online: https://www.inf.ed.ac.uk/ teaching/courses/sp/2015/lecs/BSIMM6.pdf (accessed on 30 March 2022).

217. Park, M.; Oh, H.; Lee, K. Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors 2019, 19, 2148.

218. Romano, N. Securing Our Future Homes: Smart Home Security Issues and Solutions. 211. Available online: https:// digitalcommons.liberty.edu/honors/864/ (accessed on 30 March 2022).

219. H. Tan, N., Y. Wong, R., Desjardins, A., A. Munson, S., & Pierce, J. (2022, April). Monitoring pets, deterring intruders, and casually spying on neighbors: Everyday uses of smart home cameras. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (pp. 1-25).

220. Brush, A.J.; Albrecht, J.; Miller, R. Smart Homes: From Research to Industry. In IEEE Pervasive Computing; IEEE: Piscataway, NJ, USA, 2020.

221. Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016.

222. Ghirardello, K.; Maple, C.; Ng, D.; Kearney, P. 2018 Cyber Security of Smart Homes: Development of a Reference Architecture for Attack Surface Analysis. In Proceedings of the Living in the Internet of Things: Cybersecurity of the IoT—2018, London, UK, 28–29 March 2018.

223. Abdur, M.; Habib, S.; Ali, M.; Ullah, S. Security issues in the Internet of Things (IoT): A comprehensive study. Int. J. Adv. Comput. Sci. Appl. 2017, 8, 383.

224. Chitnis, S.; Deshpande, N.; Shaligram, A. An Investigative study for smart home security: Issues, challenges and countermeasures. Wirel. Sens. Netw. 2016, 8, 77–84.

225. Erfani, S.; Ahmadi, M.; Chen, L. The Internet of Things for smart homes: An example. In Proceedings of the 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Bangkok, Thailand, 16–18 August 2017.

226. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411.

227. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. IEEE Commun. Surv. Tutor. 2014, 16, 1933–1954.

228. Ali, W.; Dustgeer, G.; Awais, M.; Shah, M.A. IoT based smart home: Security challenges, security requirements and solutions. In Proceedings of the 2017 23rd International Conference on Automation and Computing (ICAC), Huddersfield, UK, 7–8 September 2017.

229. Camacho Cruz, H.E.; González Mariño, J.C.; Foullon Peña, J.H. Parallelization Strategy Using Lustre and MPI for Face Detection in HPC Cluster: A Case Study. Comput. Sist. 2020, 24, 189–199.

230. Tian, F.; Gao, B.; Cui, Q.; Chen, E.; Liu, T. Learning deep representations for graph clustering. In Proceedings of the AAAI Conference on Artificial Intelligence, Québec City, QC, Canada, 27–31 July 2014.

231. Koutsaki, E., Vardakis, G., & Papadakis, N. (2023). Spatiotemporal data mining problems and methods. Analytics, 2(2), 485-508.

232. Koutsaki, E., Vardakis, G., & Papadakis, N. (2025). Event Prediction Using Spatial–Temporal Data for a Predictive Traffic Accident Approach Through Categorical Logic. Data, 10(6), 85.