MIDDLESEX UNIVERSITY

FINAL YEAR PROJECT

REPORT

Cybersecurity Vulnerabilities in Smart Home IoT Devices

Author

Mahie Rahman

M00804091

Supervisor

Dr Can Başkent

30/03/2025

Abstract

Smart home devices are increasingly becoming a staple item in their households due to their ease of use, energy efficiency, and automation features. However, their growing inclusion into everyday life brings many different cybersecurity vulnerabilities, which are often not addressed or are pushed aside while designing these devices. This report explores the widespread vulnerabilities in smart home IoT devices, including weak default credentials, insecure communication protocols, and poor data privacy measures. By examining real-world attack vectors, such as the Mirai botnet, and an analysis of the current mitigation strategies, this report highlights the urgent need for improved security solutions in IoT ecosystems. The findings emphasise that present solutions are often inadequate and propose novel frameworks for enhanced protection, including hardware-based security mechanisms, network-level monitoring, and cross-industry collaboration. The report concludes with recommendations for future research and practical implementations.

Keywords: Smart Home, IoT, Cybersecurity, Vulnerabilities, Privacy, Intrusion

1 Table of contents

Contents

Abstract 2
1 Table of contents 3
2 Declaration 5
3 Acknowledgement 6
4 Introduction 7
4.1 Problem Definition 7
4.2 Report Structure 8
4.3 Aims 9
4.4 Objectives 10
4.5 Deliverables 10
5 Background and Literature Review 11
5.1 Smart Home IoT Ecosystems 11
5.2 Cybersecurity Vulnerabilities in Smart Home Devices 15
5.3 Threat Models and Attack Vectors 18
5.4 Case Study: The Mirai Botnet – A Turning Point in IoT Security Awareness 20
5.5 Privacy Implications in Smart Homes 25
5.6 Security Frameworks and Their Limitations 27
5.7 Summary and Research Gaps 28
6 Problem Description and Problem Statement 29
6.1 High-Level Problem Presentation 30
6.2 Why the Problem Is Important 31
6.3 Constraints and Assumptions 32
6.4 Problem Statement 33
7 The CIA Triad in Smart Home IoT Security 33
7.1 Threat Models for Smart Home IoT Systems 36
7.2 Layered Threat Analysis Model 37
7.3 Security-by-Design and Privacy-by-Design Principles 39

7.4 Risk Assessment and Compliance Frameworks in Smart Home IoT 41
8 Description of Approach and Method(s) to Solve the Problem 44
8.1 Research Design 44
8.2 Sources and Data Collection 45
8.3 Analysis Method 45
8.4 Justification of Methodology 46
8.5 Limitations of the Approach 47
9 Results 47
9.1 Overview of Key Findings 48
9.2 Summary Table of Vulnerabilities and Responsible Stakeholders 49
9.3 Interpretation of Results 50
10 Conclusions 51
10.1 Summary of Findings 51
10.2 Achieving Project Aims 54
10.3 Final Reflections 57
11 Evaluation and Discussion 59
11.1 Evaluation of methodology 59
11.2 Strengths and limitations 60
11.3 Broader impact of the Findings 61
11.4 Future Work 62
11.5 Conclusion of Future Work 64
12 References 64

2 Declaration

I hereby confirm that the work presented here in this report and in all other associated material is all my own work.

3 Acknowledgement

I would like to thank my supervisor Dr Can Başkent for his guidance and encouragement throughout this project. I also acknowledge the support of the Learning Enhancement Team and the Middlesex University library staff for their assistance with research and academic writing.

4 Introduction

The integration of Internet of Things (IoT) technologies into home environments has transformed the traditional home into a dynamic, networked ecosystem widely referred to as a smart home. The smart environments leverage IoT devices: smart thermostats, security cameras, lighting controls and systems, voice assistants, and electronic door locks such as Ring. These enhance user comfort, efficiency, and control. However, the increasing number and diversity of these devices raise substantial cybersecurity concerns.

Unlike traditional computing devices, IoT smart home products are often resource-constrained, designed for cost-effectiveness, and deployed with minimal consideration to security. This lack of standardisation and regulation creates a rich ground for cyber threats. As the adoption of these devices grows, so does the possibility for them to be exploited as attack vectors. The expanding attack surface, when combined with low user awareness and default configurations that are not adequately secured, constitutes an environment that is vulnerable to unauthorised access, data breaches, and even physical intrusion.

This report addresses these pressing cybersecurity challenges by examining the vulnerabilities found in smart home IoT devices and proposing mitigation strategies to reduce the associated risks.

4.1 Problem Definition

Despite the rapid uptake of smart home technology, security factors often become a secondary issue in many consumers Internet of Things (IoT) products. Businesses tend to prioritise making their products available fast and user-friendly over security features. Consequently, products are shipped with insecure default settings, no remote updating available for them, and obsolete communication protocols that do not protect their data. It’s that lack of care that leaves consumers with greater vulnerability for cybersecurity issues.

Another major issue is that the IoT devices are inter-connected. The smart home usually includes products made by different manufacturers, and they have their own security policies. Since there are many setups and they don't have a common security policy, it becomes difficult to defend the smart home. And most of the users are not technical enough in setting up their devices in a secure way, making the attacks likely.

Real incidents such as the 2016 Mirai botnet attack demonstrate just how simple it is for malicious people to hijack internet of things devices for criminal activities. Also, internet of things products has access to private personal data, such as audio and video recordings, and daily routines, prompting bigger privacy concerns.

The most notable challenge that this project aims to address is that of weak IoT device cybersecurity in smart homes. This vulnerability jeopardises the security, privacy, and trust of users. The project will explore what kinds of attacks target IoT devices, review existing methods of defending themselves from such attacks, and propose improved solutions to render them secure.

4.2 Report Structure

This report contains several chapters. There are constructed to follow one after the other and assist the reader in comprehending the cybersecurity challenges of smart homes.

Chapter 4: Introduction – This chapter provides background, describes the problem, outlines the goals and objectives, and illustrates what will be created by the project.

Chapter 5: Background and Literature Review – Reviews research on Internet of Things device weaknesses. Discusses the types of attacks, prevention methods, and why rules and regulations are required.

Chapter 6: Problem Description and Problem Statement – Discusses particular security issues of smart homes, describes the boundaries of the problem, and outlines the rules and assumptions of the research.

Chapter 7: Theory – This chapter describes concepts such as the CIA triad (Confidentiality, Integrity, Availability), threat modelling, and security-focused IoT architecture.

Chapter 8: Methodology – Discusses how research was conducted to identify, review, and analyse problems of smart home systems.

Chapter 9: Results – Presents findings from the case studies, simulations, or assessments of existing security procedures.

Chapter 10: Discussion and Evaluation – Discusses the findings regarding the problem, mentions any limitations, and examines the broader repercussions.

Chapter 11: Conclusion and Future Work – This section concludes the work, reiterates its contributions, and recommends areas for future research and development.

Every chapter is authored with an objective of making the reader understand the subject matter, guiding the reader from the problem right through to the solution.

4.3 Aims

The central aim of the work presented is to thoroughly examine the security issues of smart home Internet of Things networks and determine the most effective ways of solving them. This involves identifying security vulnerabilities prevalent in these networks, understanding why and how they are exploited, and examining how effective existing preventions are under real-world conditions.

One other aim we have is to bridge the gap between cybersecurity professionals and common individuals by providing understandable and simple-to-comprehend information. Through this project, it is hoped that recommendations can be made to improve the security of existing devices and influence best practices in future IoT development.

The project also aims to advance the academic discourse on IoT cybersecurity by integrating perspectives from computer science, network security, and privacy law, thereby offering a multidisciplinary approach to a problem of increasing importance.

4.4 Objectives

To fulfil the aim outlined above, the project sets out the following specific objectives:

1. To identify and categorise common security vulnerabilities in smart home IoT devices.
   This includes an exploration of firmware issues, communication protocol weaknesses, unsecured APIs, and physical tampering risks.
2. To review current academic and industry literature on smart home cybersecurity.
   This will help to understand the state-of-the-art in threat detection, prevention, and user-level security awareness.
3. To analyse real-world attack scenarios involving smart home devices.
   Case studies will be examined to demonstrate the practical implications of poor security practices and the effectiveness of different countermeasures.
4. To evaluate the current security architectures used in consumer IoT ecosystems.
   This involves assessing the role of hubs, mobile apps, cloud infrastructure, and third-party integrations in system-wide security.
5. To propose design and policy recommendations that enhance the security posture of smart home IoT environments.
   These may include technical solutions (e.g., automatic patching, encryption standards) as well as user-cantered practices (e.g., simplified security configurations).

4.5 Deliverables

The expected outcomes and tangible outputs of this project are as follows:

- Comprehensive literature review – A critically evaluated body of research covering academic papers, industry whitepapers, and case studies on smart home security.
- Threat landscape analysis – A documented overview of known and emerging threats, mapped to specific device categories and attack surfaces.
- Case study evaluations – In-depth reviews of real-world incidents where smart home devices were exploited, detailing how the attacks occurred and their impact.
- Security framework recommendations – Practical suggestions for improving device-level and network-level security, targeting manufacturers, policymakers, and consumers.
- Final report document – A professionally formatted academic report presenting all findings, methodologies, and conclusions, meeting Middlesex University's CST3990 criteria.

5 Background and Literature Review

This section provides a structured review of existing literature in the field of smart home IoT cybersecurity. It is divided into thematic areas that reflect the most relevant technical, ethical, and practical issues associated with the topic. The review is based solely on high-quality academic sources retrieved from ScienceDirect and other articles from Google Scholar, reflecting both breadth and depth of current understanding.

5.1 Smart Home IoT Ecosystems

Smart Home networks, placed in the context of the Internet of Things (IoT), refer to devices that work independently or in cooperation in domestic contexts. Representative examples of such devices include smart thermostats, light systems, security devices, doorbells, voice command interfaces, and energy monitors, which are linked through local area networks (LANs) or cloud infrastructure. The most important functions of these devices consist of comfort improvement, efficiency maximisation, and security enhancement through the collection of information, the

undertaking of actions upon implementation of protocols, and remote control through mobile applications (Tahsien, Spachos, & Karimipour, 2020).

These smart devices typically communicate with each other through a number of communication protocols based on Zigbee, Z-Wave, Bluetooth Low Energy (BLE), and Wi-Fi. Although such multiplicity provides design flexibility in the system, it also creates significant security, compatibility, and scalability challenges. According to Alsakran, Bendiab, Shiaeles, and Kolokotronis (2021), there are many consumer-grade smart devices that have limited computational capacities, making the application of traditional security features such as thorough encryption or real-time anomaly detection impossible, mainly due to limitations in processing capacity and energy.

A key attribute of smart homes includes their reliance on cloud computing technology. Many of the entities of the Internet of Things (IoT) industry have their data stored and device updates handled using cloud infrastructure. Even though this reduces the computational load on individual units, it fosters a reliance on outside systems and the associated risks (Alrawais, et al., 2017). Also, the usage of proprietary protocols by different manufacturers creates heterogeneous ecologies with no central control, thus making whole-system security analyses harder (Morgner, et al., Opinion: Security Lifetime Labels -- Overcoming Information Asymmetry in Security of IoT Consumer Products, 2018).

Home automation networks are usually connected by a central hub or mobile app, serving as a concentration point for setting up and command transmission. However, the user interfaces of these networks have notable differences when it comes to security measures. Some applications have multi-factor authentication and access control features, while others have remote access with limited user control options (Hammi, Hammi, Bellot, & Serhrouchni, 2018).

Current research shows that the complexity involved in integrating different devices into a network increases the chances of misconfigurations. For example, while a smart lock may be connected securely, an insecurely connected smart plug in the

same network may provide a potential entry point for attackers to later move in to the network (Kouicem, Bouabdallah, & Lakhlef, 2018).

Critical Analysis:

Foundational research on smart home devices does provide insights that are useful into technical structures however, they usually simplify the challenges in the real world that these systems may meet. Studies speculate that devices follow the universal security protocols, and that users possess technical expertise, and the interoperability issues are low. Whereas the way things are, there is extreme variability that exists within Smart Home ecosystem. These are prevalent especially in terms of device security, the knowledge a user may have and the manufacturer principles.

For example, the dependence on consumer grade IoT devices are usually controlled with limited computational resources. This means that traditional security tools, (full stack encryption, and real time anomaly detection) are not practical due to the power and processing limitations (Alsakran, Bendiab, Shiaeles, & Kolokotronis, 2021). This means that these devices are being made and sold to consumers with insufficient security, or default settings that users may not change and many default passwords are easy to guess or brute force, especially when they do not have the knowledge on how to configure these devices to be secure from cyber threats. This overdependence on consumers abilities to take charge of their security measures neglects the role of human behaviour which often contributes considerably to vulnerabilities. The assumption that all users can secure their devices themselves undermines the reality that most users lack the proper knowledge to secure devices which leads to their devices exposed to all sorts of vulnerabilities.

The fragmentation of smart home ecosystems is another critical issue that the literature often overlooks. With multiple manufacturers using proprietary protocols, devices cannot be easily centrally managed, and the security of one device can undermine the entire system (Morgner, Freiling, & Benenson, 2018). While the literature frequently recommends standardisation, it fails to fully address the

systemic problems caused by this fragmentation, leading to inconsistent security practices. This fragmentation, particularly across vendors with varying levels of security compliance, results in ecosystems where certain devices are vulnerable, while others are more secure, yet they all operate within the same environment.

In addition to this, there is a critical lack of user centric research. Some studies touch on the importance of user interfaces (UI) and mobile applications for smart devices, however only a few of them investigate how the usability and security of these interfaces affect the overall system security. There are several variations in UI security, such as some apps offering two step authentications, as others don't allow users to have even the basic user controls which leaves their devices unprotected to potential threats. The below par design of user interfaces and combination of default configurations left unchanged by users leads to more security risks (Hammi, Hammi, Bellot, & Serhrouchni, 2018). As wells as this, the inadequacy of long-term device maintenance and support such as updates and patches, due to the unavailability of IT support in residential environments magnifies these issues (Chalhoub, Kraemer, & Flechais, 2024). Unlike enterprise networks, smart homes lack centralised oversight, which means devices remain vulnerable to neglected updates and unsupervised changes.

Finally, modern technology such as AI-powered automation and digital twins introduce new and more complex risks that are not explored in the literature, these systems often operate autonomously and can open new types of attacks or become targets of machine learning attacks. Many AI powered devices and cloud-based services operate as a black box system which means the vulnerabilities in these services and systems are generally invisible to the users and traditional security measures are ineffective in detecting and alleviating these advanced threats (Alrawais, Alhothaily, Hu, & Cheng, 2017). Research on AI and cloud security in smart homes is currently insufficient to address the unique challenges posed by these technologies.

In conclusion, while the literature on smart home security identifies various vulnerabilities, it largely overlooks the real-world complications, including user behaviour, device fragmentation, and the risks posed by emerging technologies. Future research must adopt a more integrated, user-centric approach, addressing these gaps and incorporating realistic models that reflect the evolving nature of smart home IoT systems.

5.2 Cybersecurity Vulnerabilities in Smart Home Devices

IoT device weaknesses in smart homes range from hardware design through firmware structure, software application stacks, and network communications. Poor implementation of security and lack of monitoring by manufacturers are root causes of the weaknesses and render smart homes an easy and inviting target for opportunistic and advanced attackers.

At the hardware level, insecure debug facilities such as exposed JTAG or UART ports are vulnerable to third-party exploit in terms of extracting confidential data or installing third-party firmware. Lack of secure element integration and physical tamper resistance further aggravates the vulnerabilities (Vishwakarma, Lee, & Gopal, 2018). Firmware security vulnerabilities include the absence of cryptographically signed update and boot verification, enabling successful downgrade or replace attacks on the firmware (Bakhshi & Tashmur, 2024).

The application layer too isn't secure. There are many mobile applications for controlling smart devices that don't have secure authentication mechanisms and proper session handling and therefore are vulnerable to man-in-the-middle (MITM) and session hijacking attacks (Vishnuvardhan, Bandela, Bairam, & Dr. Manjula, 2024). Moreover, APIs of such applications are over-permissioned by exposing more functionality than necessary and increasing the attack surface (Li, Diao, Li, Du, & Guo, 2021).

Weak points in the network usually occur due to default settings such as open ports, insecure local communication, or applying old Wi-Fi encryption protocols such as WEP. According to (Junior, et al., 2019), hackers have used UPnP and/or SSDP to discover and exploit insecure local network devices.

Critical Analysis:

While there has been extensive variation of identified weaknesses in smart home IoT products in the literature, the literature focuses on identifying weaknesses rather than proposing practical solutions for the consumer. Encrypted communication and secure boot have most frequently been proposed, but these are irrelevant when they ignore the practical limitation of consumer hardware. Cheaper products often do not have enough processing and RAM for traditional security features like cryptographically signed updates and hardware encryption. This renders proposed solutions theoretically sound but unfeasible due to the cost and power limitations placed on manufacturers (Vishwakarma, Lee, & Gopal, 2018). The study does not bridge the gap between ideal security mechanisms and consumer hardware limitations, decreasing the practicality of the proposed defences.

A further gap of critical importance is the lack of long-term security focus. While most point-of-sale vulnerabilities are widely recognised, longevity of the device does not receive wide attention. Smart home products remain unsupported or obsolete after a few years, exposing customers to unpatched attacks and upcoming threats. Lack of long-term support and vendor accountability reduces user security and decreases trust in smart home technology. It has long been a research focus that patching and vendor accountability are necessary, but these are weakly applied in the smart home Internet-of-Things sector, which remains essentially unregulated (Bakhshi & Tashmur, 2024). Lack of long-term support and transparency of update policies also contributes towards vulnerability and exposes customers to cybersecurity threats.

Moreover, transparency from the vendor side is a pertinent matter. Lack of accountability for security vulnerability disclosure and after-market security maintenance highlights security vulnerability. Elsewhere, security certifications and

mandatory vulnerability disclosures exist in sectors like automotive or medical devices. As for internet-of-things, these remain largely unregulated with incremental progress toward applying similar schemes of certification (Bakhshi & Tashmur, 2024). Lack of government agency regulation gives manufacturers room for prioritising market demand over device security, further cementing a regime in which user security becomes secondary to profitability. Without security mandates or accountability, manufacturers have no interest in keeping privacy and security in devices.

Finally, most research overlooks the human factor of smart home IoT security. Technical weaknesses like insecure debug interfaces and open ports are addressed extensively, but user behaviour remains secondary. Users use default passwords, do not install security patches, or fail to change unsafe parameters due to badly designed interfaces. Most applications do not provide fine-grained security features or explicit security alerts, resulting in minimal interaction with security-critical features from users (Vishnuvardhan, Bandela, Bairam, & Dr. Manjula, 2024). Research assumes that users are vigilant, but in fact, security habits are sporadic, especially among users with limited technical skills. Lack of consideration of user behaviour in security solutions results in impractical solutions for real-world problems. This gap recognises the necessity of a more user-centric approach with simplicity and usability as objectives.

In sum, the literature provides insightful details regarding device-level weaknesses but none of them provides end-to-end solutions in the context of daily users' problems. Future research should focus on the implementation of human factors, encouraging manufacturers' long-term security investment as well as regulatory frameworks for security certification to induce manufacturers to emphasise long-term security over short-term sales.

5.3 Threat Models and Attack Vectors

To gain an understanding of how attackers infiltrate smart home IoT configurations, we must first be aware of threat models and their associated attack vectors. Threats range from passive through active utilisation of device, and network-level weaknesses, with motivations that include monetary profit, espionage, and mass disruptions.

(Fereidouni, Zalai, & Fadeitcheva, 2025) categorise threats under passive and active types. Passive threats never intervene in the operations of the device but typically include monitoring of communications or metadata collection. Examples include listening in on unencrypted communication and monitoring device usage patterns. Active threats, however, include interference, for example, injecting malicious commands, making man-in-the-middle (MITM) attacks, or launching Distributed Denial of Service (DDoS) attacks.

A particular point of vulnerability with such vectors includes lateral movement, where an intruder gains access through an unsecured device and uses that as a starting point from where they can access other security-critical devices on the network (Morgner, Mattejat, & Benenson, All Your Bulbs Are Belong to Us:, 2017). For instance, compromised light bulb exploit could be utilised for scanning through the network before ultimately going on for use with a smart lock or surveillance system. Botnets like Mirai have indicated that potentially millions of insecure consumer Internet of Things products could be compromised for implementation in mass-volume DDoS attacks (Morgner, Mattejat, & Benenson, All Your Bulbs Are Belong to Us:, 2017).

Additionally, there are also physical assaults. Devices installed in unshielded positions (external sensors, for example, or garage installations) can be physically tampered with in the aim of circumventing authentication mechanisms or reading hardware secrets. Kumar et al. (2019) detail how proximity attacks like relay attacks and signal jamming may be used by attackers in their attempt to disrupt communication between central hubs and devices.

New threats today include adversarial machine learning, whereby the behaviour of AI-powered smart helpers or automation tools is manipulated and controlled by attackers. It remains difficult to discover and defeat such attacks due to the black-box nature of most commercial software programs (Vassilev, Oprea, & Fordyce, 2025).

Critical Analysis:

While literature distinguishes threats as passive and active, the social engineering-technical exploit hybrid model remains most often neglected. Spoofing or phishing of device pairing via voice command, for example, manages to compromise systems using merely minimal technical tools. Voice aids and customised routines increasingly rely on smart homes, and such socio-technical threats must be accorded prominence in the research of the future.

Moreover, not many threat models with an enterprise base easily map over to the domestic setting. They are contingent on IT support and central control, which are not usually present in smart homes. Threat models overlook factors such as unwatched installations and multi-household users, where various aspects of trust and careless configuration habits promote vulnerability.

One of the largest research gaps that exist today is not considering third-party cloud threats. The majority of Internet of Things products depend on third-party platforms with obscure security policies. Third-party providers' transparency and accountability gaps render them susceptible to their data breaches and remote attacks, but these are not typically reflected in threat models that already exist.

Besides, adversarial machine learning attacks on artificial-intelligence-powered smart assistants remain inadequately addressed. Since the systems are black box based, their operations could be manipulated by the attackers with flexibility, but these threats had not garnered enough attention in the literature before (Vassilev, Oprea, & Fordyce, 2025).

Finally, user behaviour remains underestimated in threat models. Modelling assumptions regarding users following sound security practices in a faithful manner ignore the prevalent issue of default credentials and insufficiently managed devices. With the rise of interconnected devices, the human element remains a extensive source of vulnerability that remains underestimated in the current research.

Most importantly, today’s threat models do not consider socio-technical factors, cloud threats, adversarial machine learning, and real user behaviour. The new models must account for these factors so that they can propose more effective and realistic security solutions for smart homes based on IoT.

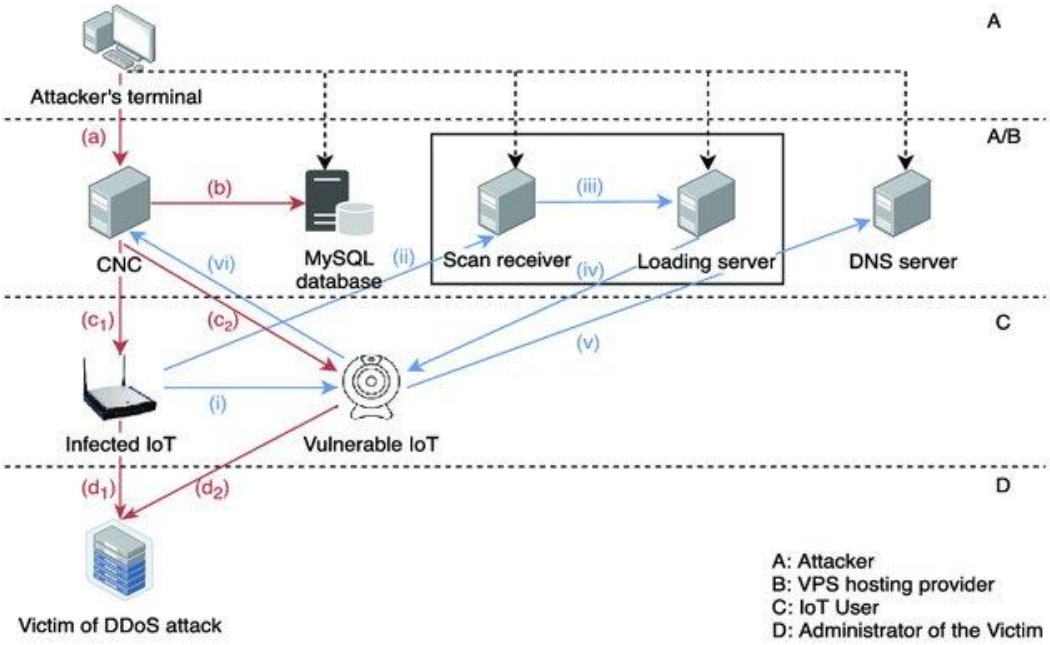
5.4 Case Study: The Mirai Botnet – A Turning Point in IoT Security Awareness

The 2016 Mirai botnet incident serves as an important milestone in smart home Internet of Things security. The malware scanned for and compromised thousands of insecure consumer-level IP cameras and domestic routers by looking for open Telnet ports and accessing them with hardcoded or default manufacturer passwords. Infected devices were enlisted into a botnet that waged historic Distributed Denial of Service (DDoS) attacks, one of which temporarily shut down major internet services Twitter, Reddit, and Netflix (Antonakakis & April, 2017)

This vulnerability that facilitated such an attack: default passwords and unsecured remote access, remains widespread among today's smart household devices. Antonakakis & April, (2017) demonstrated that Mirai has not only spread rapidly but also on its own due to a combination of the lack of basic security measures among embedded devices and the fact that the firmware is not automatically updated. This is most prevalent in smart household networks where convenience in installing them trumps secure installation.

Documented by (Affinito, Stanco, Botta, Ventre, & Zinno, 2023), the Mirai botnet revealed a deep flaw in the architecture and life cycle of smart devices: the lack of secure-by-design principles, minimal post-sales maintenance, and vendor

accountability. Even when the source code of the botnet was made available for public consumption, with subsequent versions like Hajime and Okiru emerging, there was no response from most of these manufacturers in terms of timely patches, let alone architectural redesigns.



1. Attacker's Terminal (A):
    - The attacker initiates the process from their terminal. They send commands to the command and control (CNC) server (b), which will coordinate the attack.
2. CNC Server:
    - The CNC (Command and Control) server is responsible for managing the attack. It communicates with the MySQL Database (ii), likely storing information about the infected devices and attack instructions.
    - The CNC uses the Scan Receiver (iii) and Loading Server (iv) to distribute tasks or exploit vulnerabilities in devices.
3. VPS Hosting Provider (B):

- A VPS (Virtual Private Server) hosting provider is used by the attacker to host malicious infrastructure (such as servers) which are utilized to carry out the attack. This could provide anonymity for the attacker, masking their true location.

4. IoT User (C):
    - Infected IoT devices (c1) are compromised by the attacker, turning them into botnets. These IoT devices can be anything like smart cameras, routers, or other internet-connected devices that have weak security. The attacker can now control them for the DDoS attack.
    - Vulnerable IoT (c2) devices are the ones that are easy targets for compromise due to security flaws.
5. Victim of DDoS Attack (D):
    - The victim's server (d1, d2) becomes the target of the DDoS attack. The aim is to overwhelm the victim’s server or network with massive traffic, causing it to crash or become unreachable, making the website or service unavailable to legitimate users.
6. DNS Server:
    - The DNS (Domain Name System) server (v) may be part of the attack infrastructure. DNS servers translate domain names into IP addresses, and if compromised or overloaded, they can cause disruption in accessing legitimate services.

Steps of the attack:

- The attacker uses their terminal to control the CNC server, which manages compromised IoT devices (botnets).
- The infected IoT devices flood the victim's server with traffic, leading to a denial-of-service.

- The DDoS attack could be facilitated through various servers like the Scan Receiver, Loading Server, and the DNS server.
- The vulnerability of IoT devices plays a crucial role in enabling these attacks, as attackers often exploit weak security in these devices.

This schematic emphasizes how insecure IoT devices are exploited in DDoS attacks and how attackers use a distributed network of compromised devices to target and overwhelm victims.

Critical Analysis:

Mirai botnet attack was a clear indication of the structural weaknesses in the IoT environment, particularly for consumer-grade products. The attack reflected the difference between cybersecurity knowledge and how the product life cycle is handled. The majority of IoT products have insecure-by-design aspects such as default credentials, lack of firmware update, and lack of simple security mechanisms. The unpatched and unsupported products pose risks to consumers from the time they are dispatched. Too much attention on marketability and usability for long-term security provides an environment where products are made for convenience, not security. Insecurity from day one makes it simple for attackers, as in the instance of the Mirai botnet attack.

Above all, the Mirai attack proved that smart home security threats extend beyond the individual. Devices from several private residences were hacked in order to perform gigantic DDoS attacks that affected global internet infrastructure and caused outages for necessary services such as Twitter, Reddit, and Netflix. The attack proved an invaluable lesson: with interconnectedness of IoT devices, vulnerability in even the most seemingly harmless device will be able to be utilised in order to affect global damage. What was once understood as a localised threat is now of global cybersecurity relevance, and therefore, smart home security is of public concern. With that said, however, the industry still downplays the overall risks that vulnerable IoT devices pose and instead remains steadfast in addressing market demand and convenience over remedying such glaring security weaknesses.

Unveiling the lack of regulation of the IoT marketplace. Although security for the IoT has gained a higher profile during recent times, actions like that of the UK's Product Security and Telecommunications Infrastructure Bill have done little to influence the marketplace. Too many manufacturers remain using hardcoded credentials, lack secure boot mechanisms, and disable automatic updates. Even after the Mirai attack, there was little regulatory pressure for security-by-design enforcement mandates or for post-sale support of products. This lack of regulation gives manufacturers a way around accountability for the security vulnerabilities of their products and has created a marketplace where security is an afterthought that can be ignored if the device works on the day of sale.

Additionally, the human factor of smart home security remains largely disregarded. The Mirai attack, in part, was successful because users have not changed default passwords - that vulnerability exists today in the IoT market. Failure to account for user action when creating and deploying smart home products remains an underlying challenge. Companies remain focused on convenience and choose minimalist user experiences that exclude necessary security practices (Hammi, Hammi, Bellot, & Serhrouchni, 2018). Relying on end-users to act on their behalf in advance of securing their products remains a false assumption and an ongoing industry-wide denial of the part that user action plays in security for their products. With integrated and more sophisticated IoT products becoming the norm, user education and user-friendly security alerts must be a top priority and not an afterthought.

Overall, the Mirai botnet attack was not an isolated incident but a damning indictment of an industry that continues, after all these years, to prioritise convenience and profit over security. It illustrated the degree of systematic weaknesses within the IoT environment that are heightened by vendor smugness, regulatory lack of concern, and user obliviousness. Until the industry focuses on radical design overhaul, stricter regulatory frameworks, and security features that are accessible to users, we will continue to experience cybersecurity failures that threaten not only individual users but also the integrity and soundness of global digital infrastructure.

5.5 Privacy Implications in Smart Homes

Not only do Internet of Things (IoT) smart home products enhance consumer convenience and automation but also pose serious privacy risks. There are typically ongoing captures of, transmission of, and storing of consumer information by smart home products, for example, behavioural habits, location, audio recordings, video streaming, and biometric data. Compared to traditional contexts of computing, the covert and inconspicuous nature of smart home technology keeps consumers less aware of the extent of the associated captures of data (Magara & Zhou, 2024).

(O'Connor, Jessee, & Campos, 2021) identify that privacy threats have their root in three main sources: insecure transmission leading to leakage of data, vendor data harvesting, and inferred data indirectly. Even metadata like frequency of usage and time stamps have the potential of revealing intimate home habits, presence schedules, or user preference. For example, the energy consumption from smart meters may be harnessed for forecasting appliance usage, or resident presence.

(OConnor, Jessee, & Campos, 2021) refer to the challenge of centralised control of data, as most smart home technology relies on cloud services for storing and analysing data. These services are usually hosted by third parties in a foreign jurisdiction, which raises cross-border flows of data as well as inconsistencies in regulations. Additionally, there is usually no transparency regarding the time for which the data should be retained, how the data will be commodified, or whether the data will be forwarded to advertisers or law enforcement.

These privacy challenges are heightened when the products are connected via voice assistants, which constantly listen for activating words. The systems can record personal conversations by accident, retain voice recordings for extended periods, and even record background noise as commands incorrectly (Malkin, Egelman, & Wagner, 2020).

Critical Analysis:

There has been extensive work on protecting data in transit and at rest but not on controlling and consent of users for IoT smart home devices. Privacy control panels are buried, unintuitive, or not available, and their users cannot manage their data. The systems typically expect their users to read the privacy terms, but legal jargon and complexities discourage meaningful interaction (Liu, 2014). This omission disfranchises users and entrenches privacy risks.

In addition, co-habitation environments (e.g., family members or roommates) are not dealt with by privacy models. One user's device setting may unknowingly invade the privacy of another user, for instance, shared security features or assistive tools. Privacy research today assumes homogeneous privacy expectations for users, ignoring the complexities of shared dwellings.

Another privacy gap that is necessary is the lack of transparency of data sharing, monetisation, and retention with third-party institutions. Most of the smart home platforms retain their data on cloud services with clear policies for neither data sharing with advertisers and law enforcement authorities nor data monetisation, nor data retention (O'Connor, Jessee, & Campos, 2021). The global scope of these services also makes regulation and privacy of users over borders more difficult.

Lastly, while the convenience of voice assistants is immense, they harbour great privacy risks. The devices listen constantly, and they have a predisposition of recording intimate conversations and keeping them in perpetuity, with the users unaware when they are recording them (Malkin, Egelman, & Wagner, 2020). That there remains no transparency and control over voice information works to heighten privacy risks.

In conclusion, while there are technical solutions available, privacy controls that are simple and accessible for consumers remain elusive. Simple privacy architectures, readable controls, and stronger regulatory enforcement must be the focus of research for protecting consumers in more interconnected and transparent smart homes.

5.6 Security Frameworks and Their Limitations

In response to the looming security challenges of smart home Internet of Things environments, several technical frameworks have been proposed in research and industry publications. Lightweight cryptography, context-aware access control models, machine learning IDS, and distributed ledger technology such as blockchain are some of them. Practical deployment and usage of these frameworks in real life for their home environment, however, are few.

A widely marketed option is the implementation of lightweight cryptographic algorithms tailored for constrained devices. Elliptic Curve Cryptography (ECC) and block ciphers such as AES-GCM are regularly advocated based on their low computational overhead (Alrawais, Alhothaily, Hu, & Cheng, 2017). Despite their promise, implementation obstacles such as hardware incompatibility and unavailability of firmware remain prevalent in an overwhelming majority of consumer products (Phan, Linh-An, Kim, & Taehong, 2020).

Access control mechanisms have also moved from static password models towards more context-dependent models. The models adapt access rights based on context-dependent factors such as time of day, place, and user actions. While based on sound principles, such access control mechanisms are not enabled on consumer smart home application user interfaces, and that has held their uptake back (Jang & Yi, 2019).

Blockchain has gained substantial attention as a strong contender for decentralised verification and integrity of data. Studies such as Dorri et al. (2017) detail how private blockchains can bring transparency for data transactions and tamper-proofing. However, limitations with speed of processing, scalability, and energy consumption make blockchain unsuitable for applications in most low-cost devices without optimisation.

Machine learning IDS solutions are also on the rise with the promise of detecting anomalous behaviour by observing network traffic or device usage patterns. Low-resource anomaly detection solutions that could be implemented on a home router

are outlined by (Alwaisi et al., 2024). Even so, these do require labelled data, algorithmic adjustment, and computational capacity that may be higher than what exists in present-day home network gear.

Critical Analysis:

While there are numerous frameworks outlined in the literature, there remains a low rate of consumer take-up. One of the biggest challenges is the usability-security balance. Consumers want their products “to just work,” and hence manufacturers are reluctant to include security features that will be a burden on the user. It’s particularly noticeable in products which are shipped with default passwords or without user-facing update facilities.

In addition, the absence of regulation has created a patchwork security environment. Since there are no standards that must be followed a sale and post-sale supports, manufacturers abandon equipment after their life cycle ends, exposing them to subsequent threats (OConnor, Jessee, & Campos, 2021).

There is also a troubling lack of long-term study. There are few studies examining the way these systems work for extended periods of time, such as several months, or under representative conditions with many users and a range of device types. Future work must prioritise practical deployment, cost-effectiveness, and user evaluation so that security mechanisms not only are technologically feasible but are also sustainable and usable.

5.7 Summary and Research Gaps

The work presented in this chapter illustrates the scope and sophistication of cybersecurity and privacy challenges in local-area smart home networks. Observations have been made on several points: device-level weaknesses, new threat models, privacy threats, and the scope of application of existing security frameworks. There may be no shortfall in innovation in technology, but in-the-wild deployment remains hampered by a lack of standardization, user interface design problems, and poor regulatory enforcement.

There exists a critical research shortfall in the lack of long-term research that measures the smart home system development and their vulnerabilities over time. There are publications that include theoretical or laboratory measurements that do not reflect real-world operational factors such as infrequent updates, end-user installation errors, or compatibility issues between multi-vendor environments.

In addition, most of the research assumes a technologically advanced user. Little attention is paid in literature to users' understanding of risk, their interpretation of device authorizations, and their usage of privacy features. Behavioral research into the dynamics of human-device interaction and their effects on security posture are limited.

Another gap is that there are no regulatory guidelines imposing post-sale security responsibilities on manufacturers. All products have limited after-sales support that doesn't match up with long-term household uptake. Policy-driven solutions must be part of research that will promote or mandate secure-by-design methodologies and durable firmware updatability.

Finally, there are not many cross-discipline perspectives. There needs to be subsequent work bringing in the ideas from psychology, HCI, law, and economics in a way that not only provides technologically viable solutions but also workable and ethical ones.

6 Problem Description and Problem Statement

This chapter presents a detailed and academically grounded discussion of the central problem this project seeks to address. The section begins with a high-level overview of the issue, followed by a justification of its importance, and concludes with a formal problem statement. It also outlines the key assumptions and constraints that define the scope and limits of this research. The chapter meets two core objectives:

1. To present the problem clearly and in detail
2. To explain why the problem is worth investigating.

6.1 High-Level Problem Presentation

Internet of Things (IoT) technology uptake in the smart home has transformed life in homes by embedding computing in everyday objects such as thermostats, lighting, door locks, and smart assistants. The technology offers convenience, automation, and optimisation of energy consumption by gathering, processing, and sending user information through wireless networks, usually linked with the cloud or mobile apps. Rapid technology uptake has not had the same degree of security design sophistication.

Most consumer Internet of Things (IoT) products are sold with minimal security features applied, minimal updating features, and insecurely authenticated mechanisms. It is not rare for devices, for instance, such as hardcoded passwords, insecure communications, and unrecognised APIs that are available for hacking by attackers (Wurm, Jacob, & Hoang, 2016). Smart homes are especially vulnerable for hacking, where breaching of one device will serve as a gateway for access into the rest of the network of the home.

Compounding this challenge is the disorganised condition of smart home networks. There are not standardised security measures and interoperability needs among devices from different manufacturers, and coordinated defensive mechanisms are therefore more or less unfeasible (Loi, Franco, Sivanathan, & Habibi, 2017). Home customers will be responsible for managing these platforms themselves, although they will not necessarily possess the technical knowledge necessary to configure firewalls, change network access rights, or verify the integrity of the firmware.

In essence, smart homes are turning into intelligent digital environments that lack the control, monitoring, and security awareness that traditionally accompanies such infrastructure. The result is one that consists of capabilities but sorely lacking when it comes to cyber resilience.

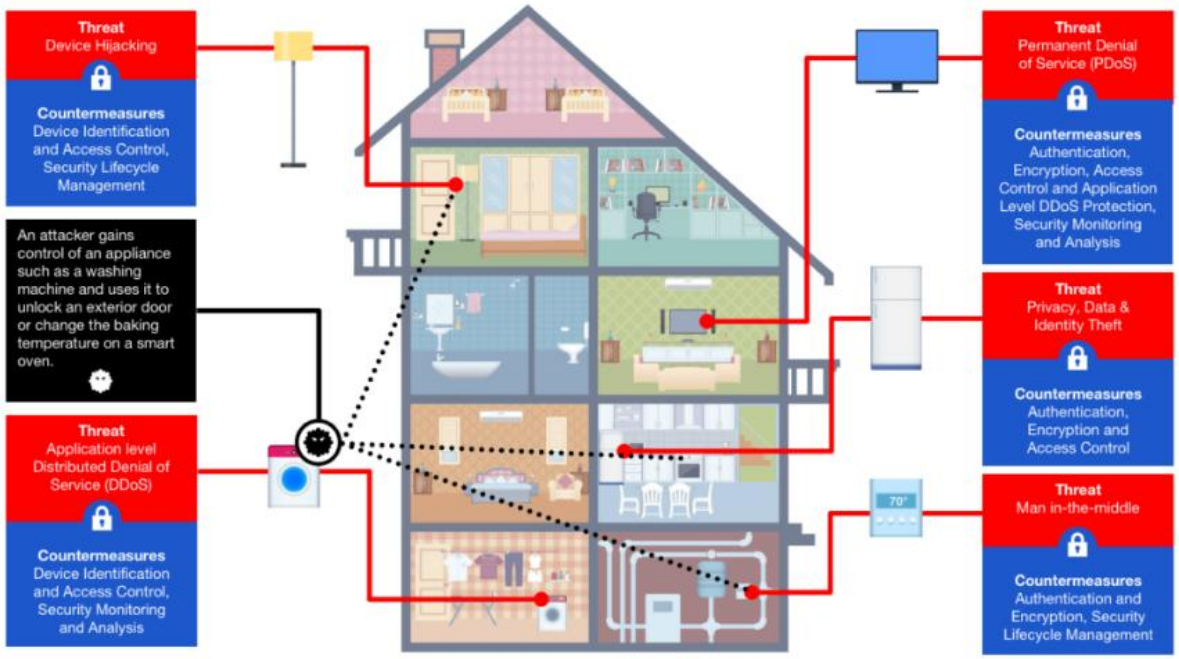
6.2 Why the Problem Is Important

The importance of addressing cybersecurity vulnerabilities in smart home IoT systems lies in their increasing integration into daily life and the sensitivity of the data they manage. Devices frequently collect video feeds, audio recordings, location data, and behavioural metrics, making them valuable targets for adversaries. A compromise could lead to stalking, extortion, identity theft, or home intrusion. (Kim, Gyubaek, Park, & Sanghyun, 2021)demonstrate how even indirect data, such as power usage or light-switch patterns, can be used to infer household activities and presence.

More worryingly, the risks extend beyond the individual. Infected devices are often used in mass attacks, like when infected home devices were used to knock down core internet infrastructure during the attack of the Mirai botnet (Antonakakis & April, 2017). As illustrated by the example, smart home insecurity isn't a domestic threat but international cybersecurity threat. (Loi, Franco, Sivanathan, & Habibi, 2017) argue that the security of the smart home must be revisited as a matter of public safety because of the threat of mass exploitation.

From an economic perspective, a lack of secure-by-design practices has downstream costs. Consumers must frequently replace devices, absorb the costs of breaches, or suffer data loss due to firmware discontinuation. Manufacturers, on the other hand, often lack legal obligation to provide long-term updates or support. This disincentivises vendors from improving device resilience post-sale.

Despite some legislative attempts such as, the UK’s Product Security and Telecommunications Infrastructure Bill, compliance across the industry remains inconsistent. Enforcement mechanisms are weak, and most regulation focuses on disclosure rather than mandatory action. As a result, consumers remain vulnerable, and the security gap continues to grow.



6.3 Constraints and Assumptions

To define the scope of this project realistically and academically, the following assumptions are made:

- The analysis focuses on consumer-grade smart home devices commonly found in residential settings (e.g., smart locks, lights, voice assistants, cameras).
- Devices are assumed to operate in typical home networks, with users acting as their own IT administrators.
- End-users have limited technical knowledge and are not security professionals.
- The study considers only documented vulnerabilities and academic research, not undisclosed exploits or forensic hardware analysis.

In terms of constraints:

- The project does not include hands-on vulnerability testing due to ethical and legal considerations.

- There is limited access to proprietary firmware or cloud backend services for detailed auditing.
- Resource and time limitations mean the analysis will primarily be literature-based and theoretical, rather than experimental.
- Findings are limited to consumer IoT devices and do not generalise to industrial or enterprise IoT systems, which follow different security protocols and lifecycle management.

These constraints define the boundaries of the investigation and ensure the research remains feasible within the timeframe and ethical scope of an undergraduate project.

6.4 Problem Statement

This project investigates the persistent and under-addressed cybersecurity vulnerabilities in smart home IoT ecosystems. It tackles the interplay between insecure-by-design products, minimal long-term vendor engagement, environment fragmentation, and minimal technical literacy among end-users. Even with mitigation techniques available, these vulnerabilities persist due to the synergetic interplay between lack of usability, poor policy enforcement, and negligence on the part of manufacturers. The goal of this work is to reveal, categorise, and critically review these vulnerabilities, and propose recommendations that bolster device strength through a combination of technical and regulatory intervention.

7 The CIA Triad in Smart Home IoT Security

The CIA triad (Confidentiality, Integrity, and Availability) is a foundational cybersecurity model that provides a structured way to evaluate and mitigate digital security risks. In the context of smart home IoT systems, the CIA principles must be interpreted through the lens of decentralised, resource-constrained, and user-managed devices that interact with both local networks and cloud infrastructures.

Confidentiality

Confidentiality involves ensuring that only the right people with proper authorisations view sensitive information. Smart home products continuously handle personal

information ranging from audio and video streams, movement patterns, and behaviour monitoring. Unsecured transmission and storage mechanisms reliably provide an opportunity for attackers to listen in on private data or gain control of private data. (Magara & Zhou, 2024) are aware that most smart home products utilise old authentication schemes and do not securely protect communications, therefore making them vulnerable to unauthorised access.

Integrity

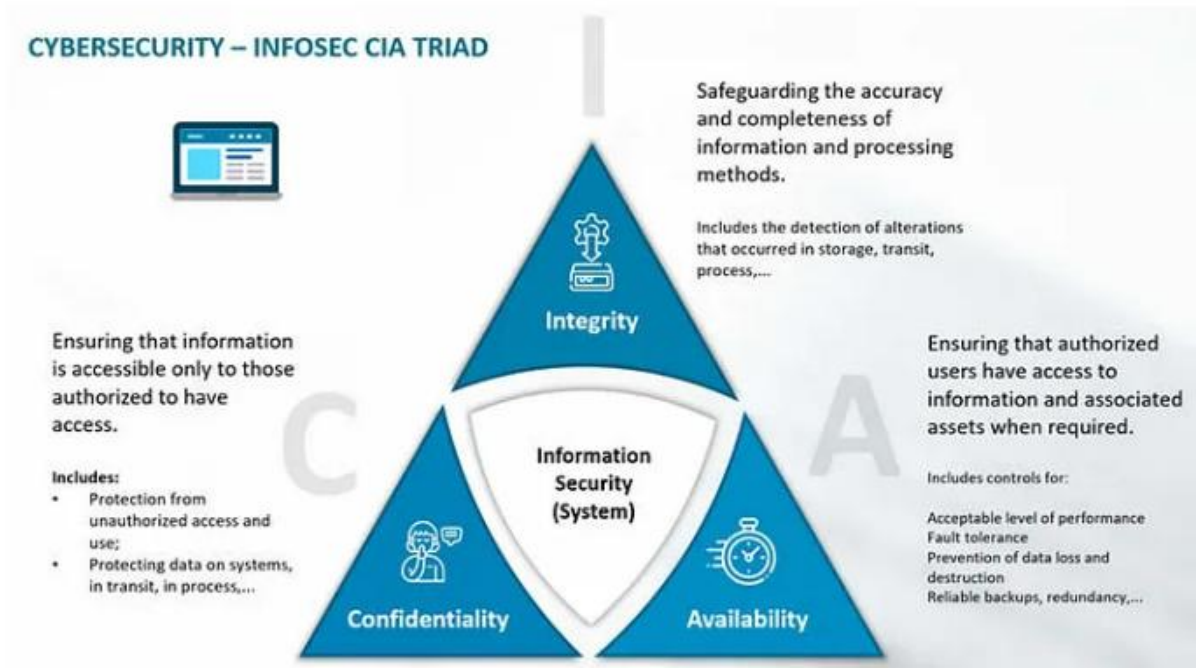
Integrity ensures that commands for the system and related data are not altered. For a smart home, which includes device commands in real time (e.g. opening a door) and stored or in-transit data (e.g. video from a motion detector). Firmware hacking and command injection will alter the intended function of devices. (Cheah, Shaikh, Bryans, & Wooderson, 2018) include among the common vulnerabilities the absence of signature verification and integrity verification in firmware updates. Integrity-violating attacks will lead to incorrect information, system malfunction, or unauthorised activity.

Availability

Availability requires that services be operational and functional when the time calls for them. For smart homes, which means that those critical devices like door locks, services, or emergency services ought to be working reliably. Because of limited computational resources and poor security design, most of the smart devices are extremely susceptible to denial-of-service (DoS) attacks. (Kim, Gyubaek, Park, & Sanghyun, 2021) that compromised the availability in smart homes, particularly in emergencies, have the potential for substantial physical or security effects.

Table 1: CIA Triad Applied to Smart Home Devices

CIA Principle	Smart Home Example	Typical Threat
Confidentiality	Video streams from IP cameras	Eavesdropping, remote access
Integrity	Firmware for smart locks/lights	Tampering, forged updates
Availability	Smart locks or alarm systems	DoS attacks, battery exhaustion



Critical Reflection:

While the CIA triad provides a solid foundation, its implementation in smart home Internet of Things (IoT) networks is marred by a host of practical limitations. On the corporate level, security measures are encoded and applied by professionals, but in the smart home environment, technically inexperienced users are responsible. This introduces a critical difference in responding to security risks, particularly with regard to areas like network segmentation, credentialing, and software updating. The "Confidentiality–Availability trade-off" manifests very easily in the smart home context, where ease of installation and deployment speed are of greater importance than robust security. For that reason, the majority of such products are dispatched with default settings or poor authentication methods, leaving them exposed to a wide range of risks (Aldahmani et al., 2023).

Besides, technical security principles preferred by the CIA model ignore human-centric factors such as cohabitant privacy, over-privileged devices, and third-party data sharing. Social and behaviour factors such as these pose top concern for smart home security but are not thoroughly addressed by the CIA model. Users themselves may remain oblivious of security implications of their behaviours or of cohabitant-

used device sharing patterns that inadvertently violate privacy. As the present research attempts to investigate both technical and behaviour-dependent vulnerability, the CIA triad provides a useful base but must be filled out by more comprehensive, integrated frameworks for addressing the multi-dimensional, dynamic character of threats in smart home security.

Link to Project Aims

The application of the CIA model supports this project's core aim: to explore vulnerabilities in smart home IoT devices and recommend design-level and policy-oriented solutions. Understanding how each principle is violated in practice provides the theoretical grounding for evaluating device behaviours and regulatory gaps in the chapters that follow.

7.1 Threat Models for Smart Home IoT Systems

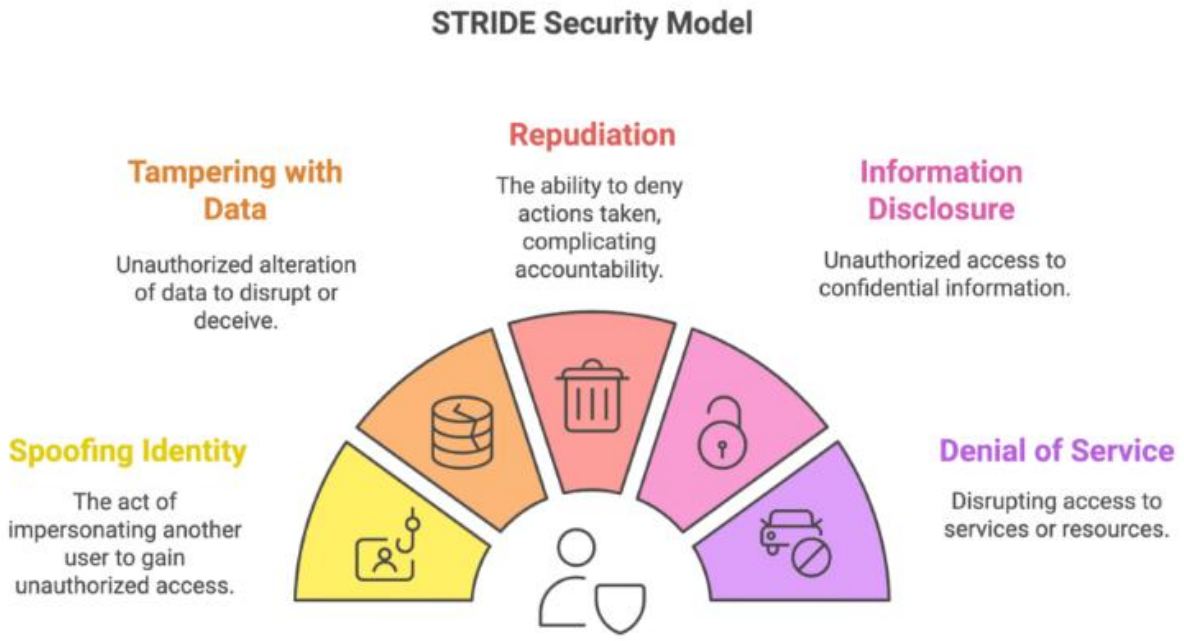
A threat model is a systematic approach towards threat identification, threat categorisation, and assessment of threats possible for a system. It requires threat modelling for smart home IoT because we must understand how attackers exploit hardware, software, network, and human factor weaknesses. Smart homes are not only resource-constrained but also decentralised, so threat models for businesses must be adjusted or supplemented according to the specific environment of a home.

STRIDE Framework in Smart Homes

The STRIDE model, developed by Microsoft, categorises threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. This model is particularly useful for evaluating threat vectors in the layered architecture of smart homes: spanning devices, gateways, applications, and cloud services.

Threat Type	Smart Home Example
Spoofing	Faking device identity (e.g., spoofed motion sensor)
Tampering	Modifying firmware to disable alarms

Repudiation	Lack of logging on device actions (e.g., no record of door unlocking)
Information Disclosure	Exposing voice logs or video feeds
Denial of Service	Overloading smart hubs to disable all devices
Elevation of Privilege	Using a basic smart plug to gain access to router-level controls



While STRIDE provides a full taxonomy, in smart homes its implementation usually finds that the devices do not have monitoring, logs, and control over privileges for detecting or preventing such threats. As most of the smart home platforms provide higher privileges to the devices that connect them without access control with granularity, they are hence exposed to lateral movement and privilege escalation, as noted by (Aldahmani, Ouni, Lestable, & Debbah, 2023).

7.2 Layered Threat Analysis Model

Besides STRIDE, layered models also give an idea of where threats are from and how they spread. (Tewari & Gupta, 2020) suggest a layer model splitting the smart

home into four layers: physical, network, application, and cloud layers. Each of these layers has its own vulnerabilities and needs extraordinary measures.

• Physical Layer: The devices can be physically accessed or reset (e.g., SD cards for cameras, reset buttons).

• Network Layer: Unsecured Wi-Fi configurations or the absence of segmentation enable sniffing and man-in-the-middle attacks.

Application Layer: Maliciously encrypted mobile applications or over-permissive applications may expose users' details.

• Cloud Layer: Remote control platforms may retain their data insecurely or with weak authentication.

This model also parallels actual attacks such as the one launched by the Mirai botnet, where initial access occurred through compromised network-facing services and paved the way for further extensive impact (Antonakakis & April, 2017).

Critical Reflection:

Although these models provide valuable structure, they are often underused in commercial smart home development. Many device manufacturers do not formally model threats during the design phase, opting instead for reactive security measures, if any at all. Furthermore, most existing models assume a technically proficient operator, whereas smart homes are typically managed by laypersons with limited cybersecurity knowledge.

Additionally, threat models such as STRIDE or layered analysis frameworks often overlook technical factors: like shared device access in multi-user households, or post-sale third-party integrations (e.g., IFTTT, Alexa Skills), which introduce novel threat vectors that cannot be easily categorised.

Thus, while threat models provide an essential foundation for smart home risk assessment, their effectiveness depends heavily on how deeply they are embedded into the design, configuration, and update lifecycle of devices.

7.3 Security-by-Design and Privacy-by-Design Principles

Smart home devices are often developed under intense market pressure to prioritise cost, usability, and speed to market. As a result, security and privacy are frequently treated as add-ons rather than core requirements. The principles of Security-by-Design (SbD) and Privacy-by-Design (PbD) provide structured approaches that aim to embed protection mechanisms from the earliest stages of development, rather than applying them reactively.

Security-by-Design in Smart Home Contexts

Security-by-Design refers to a philosophy and engineering practice where security considerations are integrated at every stage of the system development life cycle: from requirements gathering to deployment and maintenance. In smart homes, this includes measures such as:

- Implementing strong default configurations (e.g. unique device credentials)
- Providing encrypted data transmission by default
- Designing secure update mechanisms (e.g. digitally signed OTA firmware)
- Enabling least-privilege access and role separation for device permissions

(Aldahmani, Ouni, Lestable, & Debbah, 2023) argue that the lack of formal security engineering in many smart home products results in “insecure-by-default” conditions, where devices are exposed to known attack vectors even before reaching end users. This has been confirmed in multiple observed studies, including those examining vulnerable smart plugs, doorbells, and surveillance devices that lack proper access controls or permit remote access via outdated APIs.

(Yousefnezhad, Malhi, & Främling, 2020) emphasise the importance of lifecycle-aware security, noting that many vulnerabilities emerge not during the initial setup but through unpatched firmware, misconfigured cloud backends, or expired SSL

certificates. Security-by-Design thus needs to account for post-sale maintenance and assume that devices will remain in use far longer than manufacturers anticipate.

Privacy-by-Design and Data Minimisation

Privacy-by-Design complements SbD by focusing on the protection of user data. It is especially relevant in smart home environments where devices continuously collect personal, biometric, and behavioural data. PbD principles encourage developers to:

- Minimise data collection to what is strictly necessary.
- Offer transparent user controls and consent mechanisms.
- Store data locally where possible, rather than by default in third-party clouds.
- Provide granular settings to disable unnecessary data tracking.

(Kim, Gyubaek, Park, & Sanghyun, 2021) demonstrate how even non-sensitive metadata, such as lighting patterns or thermostat adjustments, can be aggregated to infer personal schedules and habits. Yet, few consumer devices offer meaningful opt-outs or transparency about what data is collected and how it is processed. This suggests a disconnect between the theoretical goals of PbD and its implementation in real-world products.

(Aldahmani, Ouni, Lestable, & Debbah, 2023) further state that PbD will not be possible if not only the option but the facilities and competence for making privacy-friendly decisions are made available. Usability plays a central role in privacy enforcement too - users will avoid security mechanisms or grant excessive privileges because of bad design of the UI/UX.

Critical Reflection

Though security by design and privacy by design are well-settled principles in both professional and academic literatures, they are poorly realised in the smart home sector. The reasons for this are several: absent regulation, economic incentives contrary to long-term support, and the view that user convenience must come before technical limitations.

A recurring thread of usability-security trade-offs runs through smart home research. SbD and PbD propose optimum designs but do not account for real users, who may not be inclined or competent enough to manage intricate configuration techniques. Somewhere, designers deliberately avoid user limitations by exchanging robustness for simplicity, like automatic connectivity of devices with open endpoints that are not secured or one-click pairing with no authentication.

For these principles to be effective in smart homes, they must evolve to incorporate human-centred security design: interfaces that guide rather than burden users, and ecosystems that reinforce security even in the presence of human error. This aligns directly with this project's objective to not only map technical vulnerabilities but also evaluate the design and behavioural conditions that allow them to persist.

7.4 Risk Assessment and Compliance Frameworks in Smart Home IoT

Smart home devices, despite their growing role in everyday life, rarely follow the same structured security risk assessment and compliance frameworks adopted in enterprise or industrial IoT settings. As the number of deployed devices rises, so does the attack surface, and without an effective framework to assess, monitor, and mitigate risks, consumers and regulators are left with incomplete visibility into potential threats.

Established methodologies such as NIST SP 800-30, OWASP Internet of Things Top 10, and ISO/IEC 27005 bring methodological techniques for security and privacy risk identification into networked infrastructure. We describe these standards in this section and critically examine their relevance and limitations in the context of the smart home.

NIST SP 800-30 – Risk Management for Information Systems

NIST SP 800-30 from the National Institute of Standards and Technology provides recommendations for the assessment of risks for an information system. It calls on the stakeholders to prioritise assets, identify possible threats and vulnerabilities,

analyse the likelihood of each threat and its size, and implement appropriate controls.

While this framework is comprehensive, its adoption in consumer IoT, especially in smart homes, is minimal. Unlike enterprise networks where IT staff can assign risk values and deploy mitigations systematically, smart home ecosystems are managed by end users with limited technical knowledge. As (Magara & Zhou, 2024) note, the decentralised nature of smart homes and the absence of continuous monitoring mechanisms make risk profiling difficult and often inaccurate.

Additionally, most manufacturers do not publish security baselines or risk matrices for their devices, further distancing smart home systems from formal compliance with NIST recommendations.

OWASP IoT Top 10

The Open Web Application Security Project (OWASP) IoT Top 10 is a widely referenced list of the most critical security vulnerabilities in IoT systems. The 2021 update includes risks such as:

- Weak or hardcoded passwords
- Insecure network services
- Lack of secure update mechanisms
- Insufficient privacy protection
- Insecure default settings

This list is especially informative in smart home environments, where these issues are most prevalent. (Tewari & Gupta, 2020) detail that most low-cost consumer goods continue to be shipped with default credentials and lack over-the-air update services, exactly reflecting OWASP’s top-ranked problems.

However, OWASP is primarily a descriptive framework, it identifies common issues but does not enforce any compliance or provide scoring mechanisms for comparing devices. This limits its use in formal risk assessment but makes it an excellent educational and diagnostic tool, especially for developers and auditors.

ISO/IEC 27005 – Risk Management in Information Security

ISO/IEC 27005 is a globally recognised standard that supports the implementation of information security based on risk management. It introduces a cyclical process of risk identification, assessment, treatment, and review. Its strength lies in its compatibility with ISO 27001 certification processes and its modular approach to different domains.

While applicable to smart homes in theory, its implementation is almost non-existent in consumer markets the cost, complexity, and documentation requirements of ISO frameworks make them inaccessible for most IoT vendors operating in cost-sensitive sectors.

Nonetheless, ISO/IEC 27005 provides a useful benchmark for what ideal security governance might look like if future legislation were to require manufacturers to maintain minimum cybersecurity standards.

Critical Reflection

Although these frameworks provide valuable structure, none are truly optimised for the smart home environment as it currently exists. They are either too technical for average users (NIST), too high-level for direct application (ISO), or too descriptive without enforcement mechanisms (OWASP). Moreover, none account for cohabitation dynamics, user misconfiguration, or post-sale device lifespan, which are critical to understanding real-world risk in smart homes.

A practical path forward may involve hybridising these standards: adopting the threat awareness focus of OWASP, the structured analysis of NIST, and the policy maturity of ISO, while scaling them down into a usable compliance checklist for developers and vendors in the consumer IoT space.

8 Description of Approach and Method(s) to Solve the Problem

This chapter outlines the methodology used to investigate cybersecurity vulnerabilities in smart home IoT systems. It includes the project approach, data sources, methods of analysis, and justification for using a literature-based research design. The methods align with the project's aims and objectives defined in Chapter 1 and are designed to critically explore technical vulnerabilities, user behaviour, and systemic weaknesses in smart home security.

8.1 Research Design

This research utilizes a qualitative, literature review design based on a critical review of literature, technical reports, and case studies. This is appropriate for the nuance and variability of IoT security as well as the ethical and legal restrictions on testing either live hardware/software or real-world systems.

Instead of experimenting with or performing penetration testing in the first instance, the project considers vulnerability and attack vectors through reading peer-review literature, such as studies and case studies of notable attacks (e.g., Ring device hacks, Mirai botnet attack). Using published works, the research avoids ethical and privacy concerns of first-hand experimenting with obtaining an in-depth understanding of smart home IoT security threats.

This approach is common in cybersecurity policy and governance research where field experiments are not possible due to ethical constraints and legal restrictions (Aldahmani, Ouni, Lestable, & Debbah, 2023). The research approach also supports ethical end-to-end analysis of the vulnerability of the Internet of Things, which keeps the research within professional and scholarly standards of research ethics.

8.2 Sources and Data Collection

The selection of sources was guided by the following criteria to ensure the relevance, credibility, and timeliness of the data:

- Relevance to smart home IoT security
- Academic credibility (primarily ScienceDirect and IEEE)
- Recency (priority given to publications from 2017 onward)
- Case study value (real incidents or system-level reviews)

Types of materials include:

- Peer-reviewed academic papers
- Cybersecurity incident analyses
- Government policy documents and standards (e.g. OWASP IoT Top 10, NIST)
- Industry whitepapers where academically reviewed sources were limited.

The literature was systematically reviewed and categorized into themes, such as firmware vulnerabilities, insecure protocols, user misconfiguration, and ecosystem fragmentation. By structuring the literature this way, I was able to ensure that each identified vulnerability and attack method was placed in the context of existing research, allowing for a more thorough understanding of the interconnected risks within the smart home IoT landscape.

8.3 Analysis Method

The thematic analysis employed in this research involved identifying recurring patterns in how vulnerabilities emerge, spread, and persist in smart home environments. This method is essential for understanding the root causes and mechanisms of exploitation within IoT ecosystems. Each finding was rigorously assessed in terms of:

- Technical Root Cause: Identifying the underlying technical issues that lead to vulnerabilities (e.g. lack of encryption, open ports, inadequate firmware validation).

- Affected Layer: Categorizing vulnerabilities based on the layer of the IoT system they impact (e.g. device, network, application, or cloud).
- Exploit Method: Understanding the methods employed by attackers to exploit vulnerabilities (e.g. credential reuse, signal spoofing, malware injection).
- Mitigation Possibility: Evaluating whether a defence mechanism exists for each vulnerability, whether it is implemented, or whether it is ignored by manufacturers or users.
- Stakeholder Responsibility: Identifying who is responsible for mitigating the risks (e.g. users, vendors, ISPs, or regulators) and how they can take accountability for the weaknesses identified.

This comprehensive thematic analysis enables a holistic view of smart home IoT security, not only identifying vulnerabilities but also providing insights into why they continue to be exploited and the role of various stakeholders in addressing these risks.

8.4 Justification of Methodology

The use of qualitative, literature-based analysis is justified by several factors:

- Feasibility: Practical experimentation with live devices would require physical access, ethical approval, and vendor cooperation where none of which are feasible within the time and scope of a final-year undergraduate project.
- Risk Mitigation: Ethical risks of scanning or probing live devices in private networks are high and could breach data protection laws or violate network usage policies.
- Relevance: Academic and industry literature already documents many IoT vulnerabilities; the value lies in synthesising and evaluating this knowledge, not re-discovering known issues.

- Breadth: Literature analysis allows the investigation of a wide range of vulnerabilities across vendors, geographies, and device types which is something that empirical testing cannot achieve within the project timeline.

The chosen methodology provides a robust framework for analysing complex cybersecurity issues while ensuring the project remains within the bounds of academic integrity and ethical standards.

8.5 Limitations of the Approach

While this approach is well-suited to the research objectives, it comes with certain limitations:

- No live testing: The lack of hands-on experimentation means the findings cannot be directly validated through empirical data or real-world testing. This may limit the practical applicability of some conclusions.
- Dependence on available research: The methodology relies heavily on existing literature, meaning that recent zero-day vulnerabilities or proprietary flaws may not be fully captured. Emerging threats and undocumented vulnerabilities may not be addressed in the literature.
- Generalization limits: The recommendations provided may not be universally applicable across all smart home devices due to differences in firmware, architecture, and user configurations. This limitation must be considered when implementing the proposed solutions in real-world settings.

Despite these limitations, the methodology remains academically rigorous and valid, providing actionable insights that are in line with the aims and constraints outlined in Chapter 3.

9 Results

This chapter presents the key findings of the literature-based investigation into cybersecurity vulnerabilities in smart home IoT devices. As this project does not involve empirical testing or primary data collection, the results are derived from a structured thematic analysis of academic literature, case studies, and industry reports. The findings are grouped into four main categories: technical vulnerabilities, user-related weaknesses, vendor and ecosystem limitations, and regulatory and policy gaps.

9.1 Overview of Key Findings

Thematic review of the literature identified a consistent chain of weaknesses and systemic issues that lie behind the vulnerability of IoT smart home environments. All of these are outlined below under four broad categories:

1. Technical Vulnerabilities

- Many smart home devices lack basic security mechanisms such as encrypted communication, secure boot processes, or firmware validation.
- Open ports, insecure APIs, and outdated protocols (e.g. Telnet, HTTP) remain common across low-cost consumer devices.
- Devices often share hardware or SDK platforms, leading to “monoculture vulnerabilities” where one exploit can affect multiple products from different brands (Tewari & Gupta, 2020).

2. User-Centric Weaknesses

- Users frequently leave default credentials unchanged or connect devices without segmenting networks or adjusting access controls.
- Poor UI/UX design in apps and setup flows encourages risky behaviours or hides key security options.
- Users are typically unaware of the data being collected or shared by devices and rarely configure privacy settings beyond defaults (Bakhshi & Tashmur, 2024).

3. Vendor and Ecosystem Limitations

- Few vendors offer long-term firmware support or patching for vulnerabilities post-sale.
- Device manufacturers often do not publish detailed security baselines, threat models, or audit logs.
- Cross-vendor ecosystems (e.g. using a Philips bulb with a Google hub and a Samsung TV) are fragmented, with no unified security policy across devices (Jang & Yi, 2019).

4. Regulatory and Policy Gaps

- Current frameworks like the OWASP IoT Top 10 and UK's Product Security Bill offer good guidance but lack enforceable compliance requirements.
- Manufacturers are not obligated to meet minimum security baselines unless voluntarily certified.
- There is limited incentive for security investment unless reputational damage or litigation is likely.

These results suggest that smart home vulnerabilities are not isolated technical faults, but the result of a broader systemic failure involving product design, user behaviour, industry practices, and policy inaction.

9.2 Summary Table of Vulnerabilities and Responsible Stakeholders

The following table consolidates key cybersecurity vulnerabilities identified in smart home IoT systems and maps them to the parties most responsible for addressing them. Understanding stakeholder responsibility is essential to achieving resilient IoT security.

Vulnerability Type	Example	Responsible Stakeholder(s)
Weak/default credentials	Admin: admin on routers/cameras	Device manufacturers, end users
Insecure firmware update process	No code signing or version validation	Device manufacturers
Lack of network segmentation	All devices on same Wi-Fi	End users, platform providers (e.g. Google)
Overprivileged app permissions	Smart lights accessing mic/camera	App developers, platform providers
No long-term patching/support	Firmware EOL after 1-2 years	Manufacturers, regulators
Unencrypted data transmission	Devices using HTTP over Wi-Fi	Manufacturers, platform vendors

Metadata leaks	Behavioural patterns inferred from logs	Manufacturers, cloud service providers
Poor user interface design	Hard-to-access security settings	Developers, UX designers

This stakeholder matrix supports the interpretation that smart home vulnerabilities are not solely technical flaws, but they also emerge from decisions made across the entire development, deployment, and usage lifecycle.

9.3 Interpretation of Results

The results indicate that cybersecurity in smart home IoT environments is shaped by more than just hardware or software flaws. Rather, it is the interplay of vendor design choices, user behaviours, and policy inaction that sustains a fragile ecosystem.

First, the decentralised and fragmented nature of the ecosystem contributes to inconsistent security implementations. A secure smart lock may still be compromised via an insecure smart plug on the same network.

Second, device manufacturers are rarely incentivised to invest in long-term security features like patch management or audit logs, especially in low-cost devices where margins are thin.

Thirdly, user behaviour remains a weak point. Without sensible interfaces, proper documentation, and warnings, users will not take simple precautions. This concurs with (Wurm, Jacob, & Hoang, 2016), in that they state that most users do not know what information they are collecting and what will be done with that information.

Finally, current policy frameworks (e.g. NIST, OWASP) are great but optional with limited real-world utilisation and enforcement in consumer markets. Are vendors going to continue under-prioritising cybersecurity until regulations play catch-up?

10 Conclusions

This study sought to investigate the cybersecurity vulnerability that exists in smart home Internet of Things (IoT) networks. From a systematic review of research articles, industry reports, and real-world case studies, the study has established technical and structural reasons for the ongoing vulnerability of these rapidly growing consumer products that are technologies.

10.1 Summary of Findings

This research has determined that consumer IoT devices used in smart homes are acutely exposed as a function of a combination of insecure-by-design, low consumer knowledge, regulatory laxity, and device fragmentation. Not only are these risks threatening security and privacy risks for isolated consumers, but it poses major risks for more substantial infrastructures. With smart homes more integrated into the fabric of everyday life and interconnected, these risks compound in severity and sophistication. The research uncovered the following key findings:

1. Widespread Use of Weak or Default Credentials and Insecure Communication Protocols

Most of these IoT products are still delivered with insecure, hardcoded default passwords that most consumers never change. Weak passwords on top of insecure communication protocols such as HTTP and legacy encryption protocols render the products vulnerable to credential-stuffing attacks, man-in-the-middle (MITM) attacks, and unauthorised access. This is not an issue with a small subset of products but a deep-seated one in the industry, from smart cameras through smart home automation systems. Failure to have secure default settings leaves users open to vulnerability right from the outset when they first connect the products onto the network. That so many products do not have end-to-end encryption as a supported option further contributes to the problem, enabling attackers to tap into sensitive audio and video streams, or remotely take control of device operations.

2. Inconsistent or Absent Post-Sale Support and Updates

Among the key issues expressed in this research is the lack of long-term vendor support. Many products are released with minimal thought for after-sales support and are therefore vulnerable to threats that occur after the life of the support. Firmware patches, a basic prerequisite for addressing newly revealed weaknesses, are not available or difficult to implement, and a dangerous security loophole ensues. Without mandatory patching infrastructures and secure update infrastructures, vulnerable products remain on the shelves for end users to be endangered long after the original sale. Added to this is the fact that the definition of a vendor security commitment is not fixed, and hence manufacturers are not necessarily predisposed towards action when weaknesses are uncovered, hence leaving end users exposed.

3. User Misconfigurations and Lack of Security Awareness

While technical weaknesses lie at the root of security of smart home products, user habits are the greatest contributor. Users do not necessarily see the security implications of insecure setups because interfaces are badly thought through, or security prompts during initialisation are weak. Default insecure setups are not adjusted, and security features like multi-factor authentication (MFA) are not enabled or are inconvenient to configure. Furthermore, there is extremely limited education of consumers on best practices of securing IoT products. So, where strong security features exist, they are breached through human mistake. The time has arrived when simple interfaces and simpler access to learning security must be made so that consumers have an easier time securing products.

4. Lack of Cross-Platform Security Standards

IoT fragmentation represents one of the biggest challenges that developers have in creating unified security solutions. Devices from different manufacturers tend not to be compatible with each other in security policy, and it becomes hard to implement uniform security protocols on the whole smart home system. An example is a smart thermostat that has advanced encryption, but a smart light bulb on the same network that doesn't have basic authentication features. Platform incompatibility offers avenues of vulnerability in the security of the whole smart home network. Without

products that are jointly developed with standardisation, security becomes impossible. It exacerbates the challenge of securing smart home networks and is thus crucial that there be industry-wide security standards.

5. Minimal Regulatory Pressure and Legal Frameworks

Another fundamental discovery is that there remain no regulations on secure-by-design principles and post-sale security responsibilities. Notwithstanding initiatives like the UK's Product Security and Telecommunications Infrastructure Bill, compliance remains piecemeal throughout the industry. There remains no norm for requiring manufacturers to be enabled in a position of delivering long-term security upkeep, as well as compliance with secure-by-design principles by default. This lack of regulation leaves room for manufacturers for prioritising cost minimisation and usability over security, leading to vulnerable-by-design products. This research identifies the necessity for regulatory adjustment in setting industry-wide minimums for security standards as well as post-sale vendor accountability.

6. The Role of Emerging Technologies in Creating New Vulnerabilities

In order to enhance the smart home environment, new technology such as digital twins and products containing artificial intelligence provide new security threats. While these provide convenience and automation, these contribute security model complexity and new attack vectors. For instance, products containing AI, such as intelligent cameras and sound aids, are vulnerable to adversarial machine learning whereby the decision-making of the artificial intelligence can be manipulated by attackers. Similarly, the more pervasive deployment of digital twins (virtual copies of hardware or systems) provides new security and privacy issues with further collection and processing of personal and behavioural data. This work underlines the necessity of keeping up with research on the interaction of these new technology with existing security, such that security keeps up with innovation in the field.

Broader Implications

These findings point to the needs of addressing smart home security in a comprehensive way. Technology alone will not do. It will take the convergence of user behaviour, vendor accountability, and government policy to have in place an environment where products can exist securely and harmoniously. The human factor, be that of user awareness and user behaviour, must be addressed alongside technology such as encryption and secure boot mechanisms. Similarly, the lack of cross-platform security standards must be addressed by enforced industry cooperation and common security protocols.

Additionally, with new technologies like digital twins and artificial intelligence becoming more integrated into smart homes, upcoming research must address the definition of adaptability in security architectures that will protect these newer technology sets while not constricting innovation. This report offers a cross-cutting security perspective towards the Internet of Things, with solutions that will ensure security, usability, and privacy. It challenges industry, regulators, and consumers to collaborate and design more secure, robust, and privacy-protecting smart homes.

Why This Matters

This research underlines that the security of the Internet of Things is not a merely technical but a societal one. As smart household units proliferate, it is not thousands but millions of units that are perhaps jeopardised, not only threatening individuals but infrastructures on a national level. If we tackle these risks with an open, multi-disciplined approach, we not only make houses intelligent but also ethical environments where privacy and security are ensured. The security of the Internet of Things in the future will depend on technology creators, policymakers, and consumers collaborating on introducing robust, scalable solutions for the multifaceted, elusive nature of these infrastructures.

10.2 Achieving Project Aims

This work contributes novelty in not only cataloging technical weaknesses of smart home Internet of Things environments but also addressing systematic issues with user behavior, vendor liability, and the decentralized nature of the IoT market. I

contribute novelty with its inter-disciplinarity of technology solutions, user behavior, and policy change advocacy in proposing end-to-end and sustainable security architectures for smart homes. The findings in this report extend beyond mere vulnerability identification; they are the building blocks for practical, end-to-end solutions that have the potential to transform how smart homes are made secure.

1. Human-Centered Security Analysis

While most of the research today focuses on technical weaknesses such as insecure communications protocols or poor credentials, there remains little attention paid to the human element. The report addresses the gap by making explicit the ways in which end-user actions, such as poor configuration habits, lack of awareness, and ignoring security best practices, exacerbate vulnerabilities. It is one of the first research reports that systematically measures how such human error could be prevented through better user education, simpler device interfaces, and more accessible security configuration.

2. Innovative Holistic Security Frameworks

Among the key contributions of the research work presented herein is the creation of an end-to-end security framework that combines the ideas of Security-by-Design and Privacy-by-Design. The concepts of these frameworks are not used in their original state but are adapted for application on the given problems facing smart homes, where numerous products from different manufacturers coexist in interactive and usually insecure environments. The proposed framework encourages homogeneous security practices ranging from device-level security up to secure network configurations and vendor accountability. Adding user behavior analysis into the framework, I am convinced that the most practical security solutions must consider interplay among technology, human beings, and vendor practices.

3. Emphasis on Long-Term Device Security

This work extends the discussion from the initial point of deployment, with a focus on long-term device security that has up until now been ignored in the past. Most smart

home devices are delivered with minimal regard for long-term security needs, rendering them vulnerable to fresh attacks after they are released. Through a close study of the life cycle of IoT devices, this work calls for mandatory long-term firmware support, regular updates, and secure update mechanisms. The work contributes by addressing the consumer IoT device life cycle, which typically ends up leaving the device unsupported and open to new security attacks after its prime time.

4. Cross-Platform Coordination and Vendor Responsibility

A least-developed field of research in smart home security is the lack of cross-platform security standards. There are many products from countless suppliers without uniform security policies, and we cannot merely have one unified defense. I focus in my research on the necessity of cross-platform collaboration for standardized security protocols between IoT devices for seamless communication and secure interoperability. To that end, I call for more vendor accountability, forcing manufacturers to employ secure-by-design methods and adhere to post-sales security protocols.

5. Policy Advocacy and Regulatory Solutions

While technological solutions are necessary, these must be backed by strong regulation frameworks. This research acknowledges the function of mandatory security regulation that enforces manufacturers to adopt secure-by-design and privacy-by-design methodologies across the entire life cycle of the product. Synthesizing gaps between regulation and compliance with suppliers, this research proposes policy interventions that can enforce manufacturers' liability for long-run security for their products. My research acknowledges the regulatory imperative for promoting security improvement, particularly in an industry where profit ahead of security has traditionally remained the prime objective.

6. Integrated User Education and Awareness

The other key contribution of my work is in highlighting user education and consumer security awareness. Where the rest of the industry focuses on technological

innovation, consumer security awareness of the Internet of Things has not gained much attention. The work focuses on the importance of educational campaigns that promote consumer security awareness of the dangers of insecure use of devices and what they can do towards preventing that threat. The contribution in such a work thus involves the development of a framework for user education that includes interactive guides, security alerts, and automated security reminders such that the users are not passive recipients of security but agents themselves towards a secure environment.

10.3 Final Reflections

Smart homes, while meant for more convenience and automation, have unfortunately become substantial attack surfaces in the digital landscape of today. The weaknesses that have been revealed in the report indicate both the intricacies of the challenges of locking down smart home IoT systems. They are not mere isolated technical weaknesses but reflect on systemic shortcomings, ranging from infirm industry standards, the absence of applicable regulation, and fragmentation in the environment. My work focuses on how these, collectively, expose consumers to everything from privacy invasion through threats on their personal security.

Research showcases the need for scalable, enforceable solutions that go beyond the technical fixes and include human factors, lifecycle disciplines, and cross-platform coordination. Technical progress like improved encryption and secure firmware updates are important but inadequate by themselves in protecting users from the more pervasive exposures. As our report considers, user behaviour, keeping default credentials, failing to update devices, and ignoring security settings is a chief facilitator of the exposures. That is where my research enters: injecting design with a focus on people into Internet of Things security solutions, not just what the devices will do but how people will use them and how education or nudges will prevent the mistakes.

Additionally, there are gaping security regulation gaps for smart home IoT. Without a regulatory environment requiring secure-by-design practices, there are no incentives

for manufacturers to take a long-term security perspective. This research calls for policy that holds manufacturers accountable for the entire life cycle of the products from secure design and timely update to transparent post-sales services. I have proposed a long-term security framework with obligatory vendor accountability and post-sales services, something that needs to be done to ensure that the products do not get obsoleted in security.

While there is further expansion of the uptake of IoT, the smart homes of the future must consider more than protecting individual devices. We must consider how we build not only secure but also usable, robust, and ethical environments. One of the most challenging aspects of effective security for successful smart home technology is interoperability between smart home products, especially between vendors and platforms. This research requires cross-platform standards that facilitate unified, seamless security for a variety of products. It also needs more cooperation between vendors and industry-wide coordination so that manufacturers cooperate to establish robust, secure ecosystems rather than individual, insecure products.

These findings also pose challenges for future research to deal with the rapid development of IoT technology, such as smart artificial intelligence-enabled devices and digital twins. As they become integral to our everyday life, they bring with them opportunities but also new vulnerability challenges for smart homes. The sophistication of new systems will require that sophisticated security mechanisms be developed that are able to deal with increasing device and adversary sophistication.

In addition, while that report provides a useful jumping off point for addressing weaknesses today, there is tremendous value in testing in the field. Field testing of consumer IoT products like smart home products in empirical research, for instance, would reveal what actual field weaknesses exist in consumer products as opposed to theoretical or laboratory testing. Additionally, consumer studies of how consumers use their smart home systems would provide a clearer view of the psychological roadblocks to security so that we can design systems that are not only less error-prone but also more usable.

Finally, one cannot overlook the ethical challenges of smart home security. As IoT sensors collect vast amounts of personal information, ethical challenges of data collection, storage, and transmission must be examined carefully. Future research must be focused on defining ethical guidelines for businesses so that they protect consumers' privacy and utilise the correct uses of data. Furthermore, with growing uses of AI and machine learning for smart homes, ethical challenges of autonomy, bias, and accountability will be tackled by regulation and open practices.

This report identifies the need for a multi-stakeholder collaborative approach towards IoT security with manufacturers, regulators, educators, and consumers. All the stakeholders have a vital role in the development of secure and robust smart home environments. Together we can address the design weaknesses of current smart home IoT security and design environments that are not only secure and safe but trusted and sustainable too.

11 Evaluation and Discussion

This chapter critically examines the research methodology, approach, and broader implications of the research. The chapter evaluates the strength and weaknesses of the methodology and critically considers how the research contributes to existing knowledge in the field of smart home IoT security and suggests avenues for further research.

11.1 Evaluation of methodology

Research methodology applied in the present research was primarily literature-based and qualitative in nature, consisting of an extensive review of literature, industry publications, cybersecurity frameworks, and case studies. While the literature approach offered an over-all view of typical weaknesses that persist, there are limitations. The literature approach offered an over-all view of typical weaknesses but lacking empirical findings from actual testing under field conditions, which would have offered more specific, first-hand details on the behaviour of the devices under field attack conditions. Field testing would have also facilitated hands-

on single vulnerability testing of smart home devices for more specific understanding of their security weaknesses.

Moreover, the study relied mainly on secondary sources, which while voluminous, may not reflect the latest vulnerabilities or emerging threats, for instance, those facilitated by emerging technology such as AI-powered smart help and 5G-enabled devices. Subsequent research could benefit from empirical techniques, for instance, penetration testing and user research, to complement findings in the literature.

11.2 Strengths and limitations

Strengths

1. Systematic Literature Review: It utilizes an extensive collection of scholarly and industry publications, with the aim of obtaining an in-depth and thorough overview of the security weaknesses in smart home IoT environments. This enabled the most common security weaknesses and the limitations of the available countermeasures to be determined.

2. Multidisciplinary: Combining insights from cybersecurity, user behavior, and policy frameworks, the research offers a wide-ranging view of smart home IoT security. Multidisciplinary research operates towards addressing the intricate, multifaceted nature of the security issues addressed.

3. Real-World Context: Case studies such as the one on the Mirai botnet and its application of compromised Internet of Things units for launching attacks provide real-world context for the theoretical work by illustrating the actual implications of insecure security protocols.

L**imitations**

1. Lack of Empirical Facts: Indeed, the research was limited by a literature review, and thus no empirical testing was possible in real life. The inability to test actual devices or performing attacks on actual environments limits the validity of some of

the findings in real life. Empirical testing could provide absolute confirmation on exploiting weaknesses in real environments.

2. Lack of Consideration of New Technologies: Home automation technology evolves rapidly so that new threats, most especially of AI-powered devices and of automatic systems, are not taken seriously enough. Technology keeps evolving, and hence the attack windows, and hence upcoming research needs to counter these new threats.

3. Generalizability: Although the research focused on consumer-grade smart home devices, the results may not be fully applicable to industry- or enterprise-grade IoT platforms, which have different security expectations, models, and lifecycles.

11.3 Broader impact of the Findings

The findings of this report emphasize the urgency of addressing a multi-stakeholder approach towards IoT security challenges. The fragmentation of the IoT smart home environment, coupled with inadequate end-user education and the lack of accountability on the part of vendors, presents fertile ground for abuse. Vendors remain most concerned with usability and time-to-market over security and therefore deploy insecure-by-design products which they abandon after they have made their initial disclosure.

This research also identifies end-users themselves as one of the root weaknesses, most typically due to poor configuration, security unawareness, and insecure default settings. Therefore, effective mitigation efforts must not only address the technical weaknesses but also deal with the human factor which is designing simpler interfaces and consumer campaigns of awareness that empower users with the tools they need to defend their own computers.

Additionally, the absence of robust regulatory frameworks deprives the industry of incentives that will facilitate securing the device after sale. While there is useful guidance available in industry guidelines such as OWASP’s Internet of Things Top 10 and NIST frameworks, their voluntary nature and unenforceability undermines their effectiveness. Legislation imposing security-by-design concepts and extended

support must therefore be sought in an attempt to nudge the smart home Internet of Things sector towards a security-orientated path.

11.4 Future Work

While the present research work gives useful observations, there are many areas where research has to be conducted in order to bridge the gaps that have emerged. Any development towards smart home IoT security must include research on technical solutions as well as policy solutions, and also research on user experience within these systems.

1. Real-World Testing and Empirical Studies

A key direction for innovation in the field is real-world penetration testing of smart home products. This could be testing products from several different manufacturers and platforms for their weaknesses in real-world systems. Researchers will conduct attacks such as DDoS, man-in-the-middle, and credential stuffing attacks on the products and see how they respond and the extent to which they are vulnerable.

Additionally, user behaviour studies could be made with the aim of further understanding how users deal with their devices, their security habits (e.g., password changing, software updating) as well as their experiences updating their smart homes.

2. Long-Term Device Security

A second focus for future research is in looking at how smart devices change over time. Most smart devices come with little post-sale maintenance, leaving them exposed to threats that only materialise after the initial release time. We can analyse how smart devices perform with regard for security over long periods of time through longitudinal studies and how manufacturers are incentivised to provide regular updates over the life of their products.

3. Strengthening Vendor security practices

According to the research, several vendors do not implement necessary security-by-design practices. Future research must deal with how best to encourage such practices right from the outset. This could include reviewing regulatory frameworks that require secure-by-design certification, as well as mandatory patch schedules and privacy protections.

4. Standardising Smart Home Security

A major problem is that there isn't a common security prerequisite for products developed by different manufacturers. The possibility of establishing a common security standard for smart home products, which will enforce a minimum-security level for every product in an environment, could be explored through further research. It includes applying standardised methods of encryption, authentication, and secure communication.

5. Enhancing User Education

Because one of the leading contributors for smart home insecurity is user behaviour, there needs to be improved user education. There needs to be new research that considers what security setups should be user-friendly and there needs to be education campaigns that make security risks more apparent and transition users from insecure default setups. This includes simpler default password updates, enabling encryption, and applying firmware updates.

6. Ethical and Privacy Implications

Because smart home products collect vast amounts of personal data, privacy aspects should also be addressed in future research. Privacy-by-design strategies should be developed that restrict the quantity of personal data collected and that allow full user control over sharing and utilisation of collected data. Since there are more AI-based products in smart homes with each day that passes, research should focus on ethical application of machine learning and avoidance of abuse of personal data.

11.5 Conclusion of Future Work

A multi-faceted approach involving empirical research, vendor accountability, user education, and policy change will be the way of the future for smart home IoT security. By tackling the technical, human, and policy aspects of security for the Internet of Things, new research will be able to build a stronger, more private, more robust smart home environment. Continued research on how security protocols will be scaled for adaptation, alongside greater vendor accountability and improved user education, will be the answer for countering the dangers of smart home technology on the rise.

12 References

Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog Computing for the Internet of Things: Security and Privacy Issues. *IEEE Internet Computing*, 34-42. doi:10.1109/MIC.2017.37

Alsakran, F., Bendiab, G., Shiaeles, S., & Kolokotronis, N. (2021). Intrusion Detection Systems for Smart Home IoT Devices:. *arXiv preprint arXiv:2101.06519*. Retrieved from https://arxiv.org/abs/2101.06519

Affinito, A., Zinno, S., Stanco, G., Botta, A., & Ventre, G. (2023). The evolution of Mirai botnet scans over a six-year period. *Journal of Information Security and Applications*, 103629. doi:https://doi.org/10.1016/j.jisa.2023.103629

Alwaisi, Z., Kumar, T., Harjula, E., & Soderi, S. (2024). Securing constrained IoT systems: A lightweight machine learning approach for anomaly detection and prevention. *Internet of Things, 28*, 101398. doi:https://doi.org/10.1016/j.iot.2024.101398

Antonakakis, M., & April, T. (2017). Understanding the Mirai Botnet. *26th USENIX Security Symposium (USENIX Security 17*, 1093--1110. Retrieved from https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Bakhshi, & Tashmur. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. *Sensors (Basel, Switzerland), 24*, 708. doi:https://doi.org/10.3390/s24020708

Chalhoub, G., Kraemer, M. J., & Flechais, I. (2024). Useful shortcuts: Using design heuristics for consent and permission in smart home devices. *International Journal of Human-Computer Studies*, 103177. doi:https://doi.org/10.1016/j.ijhcs.2023.103177

Fereidouni, H., Zalai, M., & Fadeitcheva, O. (2025). IoT and Man-in-the-Middle Attacks. *Security and Privacy*. doi:https://doi.org/10.1002/spy2.70016

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, 126-142. doi:https://doi.org/10.1016/j.cose.2018.06.004

Jang, J., & Yi, M. (2019). Determining and validating smart TV UX factors: A multiple-study approach. *International Journal of Human-Computer Studies*, 58-72. doi:https://doi.org/10.1016/j.ijhcs.2019.05.001

Junior, D., Melo, L., Lu, H., d'Amorim, M., Atul, & Prakash. (2019). Beware of the App! On the Vulnerability Surface of Smart Devices through their Companion Apps. *arXiv*. Retrieved from https://arxiv.org/pdf/1901.10062

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, 199-221.

Li, R., Diao, W., Li, Z., Du, J., & Guo, S. (2021). Android Custom Permissions Demystified: From Privilege Escalation to Design Shortcomings. *2021 IEEE Symposium on Security and Privacy (SP)*, 70-86. doi:10.1109/SP40001.2021.00070

Liu, Y. (2014). User control of personal information concerning mobile-app: Notice and consent? *Computer Law & Security Review, 30*, 521-529. doi:https://doi.org/10.1016/j.clsr.2014.07.008

Magara, T., & Zhou, Y. (2024). Internet of Things (IoT) of Smart Homes: Privacy and Security. *Journal of Electrical and Computer Engineering, 2024*, 17. doi:https://doi.org/10.1155/2024/7716956

Malkin, N., Egelman, S., & Wagner, D. (2020). Privacy controls for always-listening devices. *Proceedings of the New Security Paradigms Workshop*. doi:https://doi.org/10.1145/3368860.3368867

Morgner, P., Freiling, F., & Benenson, Z. (2018). Opinion: Security Lifetime Labels -- Overcoming Information Asymmetry in Security of IoT Consumer Products. doi:10.1145/3212480.3212486

Morgner, P., Mattejat, S., & Benenson, Z. (2017). All Your Bulbs Are Belong to Us:. doi:http://dx.doi.org/10.48550/arXiv.1608.03732

OConnor, T., Jessee, D., & Campos, D. (2021). Through the Spyglass: Towards IoT Companion App Man-in-the-Middle Attacks. *CSET '21: Proceedings of the 14th Cyber Security Experimentation and Test Workshop*, 58–62. doi:10.1145/3474718.3474729

Phan, Linh-An, Kim, & Taehong. (2020). Breaking Down the Compatibility Problem in Smart Homes: A Dynamically Updatable Gateway Platform. *Sensors, 20*(2783). doi:10.3390/s20102783

Tahsien, S. M., Spachos, P., & Karimipour, H. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, 102630.

Vassilev, A., Oprea, A., & Fordyce, A. (2025). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations.* NIST. doi:https://doi.org/10.6028/NIST.AI.100-2e2025

Vishnuvardhan, Bandela, Bairam, & Dr. Manjula. (2024). MOBILE BANKING – A CASE STUDY OF PRE-AUTHORIZATION AND POST-AUTHORIZATION ON

SESSION HIJACKING. *International Journal of Future Generation Communication and Networking*, 43-52. doi:10.58532/V3BKIT3P2CH3

Vishwakarma, Lee, W., & Gopal. (2018). Exploiting JTAG and Its Mitigation in IOT: A Survey. *Future Internet*. doi:10.3390/fi10120121

Wurm, Jacob, & Hoang. (2016). Security analysis on consumer and industrial IoT devices. *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 519-524. doi:10.1109/ASPDAC.2016.7428064

Research Ethics Screening Form for Students

Only for students on taught programmes – e.g., BSc, MSc, MA, LLM etc
NOT for PostGraduate Researchers – e.g., MRes/MPhil/PhD degrees

Middlesex University is concerned with protecting the rights, health, safety, dignity, and privacy of its research participants. It is also concerned with protecting the health, safety, rights, and academic freedom of its students and with safeguarding its own reputation for conducting high quality, ethical research.

This Research Ethics Screening Form will enable students to self-assess and determine whether the research requires ethical review and approval via the Middlesex Online Research Ethics (MORE) form before commencing the study. Supervisors must approve this form after consultation with students.

Student Name:	Mahie Rahman	Email: mr1462@live.mdx.ac.uk
Research project title:	Cybersecurity Vulnerabilities in Smart Home IoT Devices	
Programme of study/module:	Information Technology	
Supervisor Name:	Can Baskent	Email:C.baskent@mdx.ac.uk

Please answer whether your research/study involves any of the following given below:		
1. [H]ANIMALS or animal parts.	☐ Yes	☒ No
2. [M]CELL LINES (established and commercially available cells - biological research).	☐ Yes	☒ No
3. [H]CELL CULTURE (Primary: from animal/human cells- biological research).	☐ Yes	☒ No
4. [H]CLINICAL Audits or Assessments (e.g. in medical settings).	☐ Yes	☒ No
5. [X]CONFLICT of INTEREST or lack of IMPARTIALITY. If unsure see “Code of Practice for Research” (Sec 3.5) at: https://unihub.mdx.ac.uk/study/spotlights/types/research-at-middlesex/research-ethics	☐ Yes	☒ No
6. [X]DATA to be used that is not freely available (e.g. secondary data needing permission for access or use).	☐ Yes	☒ No
7. [X]DAMAGE (e.g., to precious artefacts or to the environment) or present a significant risk to society).	☐ Yes	☒ No
8. [X]EXTERNAL ORGANISATION – research carried out within an external organisation or your reseach is commissioned by a government (or government body).	☐ Yes	☒ No

9. [M]FIELDWORK (e.g biological research, ethnography studies).	☐ Yes	☒ No
10. [H]GENETICALLTY MODIFIED ORGANISMS (GMOs) (biological research).	☐ Yes	☒ No
11. [H]GENE THERAPY including DNA sequenced data (biological research).	☐ Yes	☒ No
12. [M]HUMAN PARTICIPANTS – ANONYMOUS Questionnaires (participants not identified or identifiable).	☐ Yes	☒ No
13. [X]HUMAN PARTICIPANTS – IDENTIFIABLE (participants are identified or can be identified): survey questionnaire/ INTERVIEWS / focus groups / experiments / observation studies/ evaluation studies.	☐ Yes	☒ No
14. [H]HUMAN TISSUE (e.g., human relevant material, e.g., blood, saliva, urine, breast milk, faecal material).	☐ Yes	☒ No
15. [H]ILLEGAL/HARMFUL activities research (e.g., development of technology intended to be used in an illegal/harmful context or to breach security systems, searching the internet for information on highly sensitive topics such as child and extreme pornography, terrorism, use of the DARK WEB, research harmful to national security).	☐ Yes	☒ No
16. [X]PERMISSION is required to access premises or research participants.	☐ Yes	☒ No

17. [X]PERSONAL DATA PROCESSING (Any activity with data that can directly or indirectly identify a living person). For example data gathered from interviews, databases, digital devices such as mobile phones, social media or internet platforms or apps with or without individuals'/owners' knowledge or consent, and/or could lead to individuals/owners being IDENTIFIED or SPECIAL CATEGORY DATA (GDPR[1]) or CRIMINAL OFFENCE DATA. [1]Special category data (GDPR- Art.9): ”personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”.	☐ Yes	☒ No
18. [X]PUBLIC WORKS DOCTORATES: Evidence of permission is required for use of works/artifacts (that are protected by Intellectual Property (IP) Rights, e.g. copyright, design right) in a doctoral critical commentary when the IP in the work/artifactis jointly prepared/produced or is owned by another body	☐ Yes	☒ No
19. [H]RISK OF PHYSICAL OR PSYCHOLOGICAL HARM (e.g., TRAVEL to dangerous places in your own country or in a foreign country (see https://www.gov.uk/foreign-travel-advice), research with NGOs/humanitarian groups in conflict/dangerous zones, development of technology/agent/chemical that may be harmful to others, any other foreseeable dangerous risks).	☐ Yes	☒ No
20. [X]SECURITY CLEARANCE – required for research.	☐ Yes	☒ No
21. [X]SENSITIVE TOPICS (e.g., anything deeply personal and distressing, taboo, intrusive, stigmatising, sexual in nature, potentially dangerous, etc).	☐ Yes	☒ No

M – Minimal Risk; X – More than Minimal Risk. H – High Risk

If you have answered 'Yes' to ANY of the items in the table, your application REQUIRES ethical review and approval using the MOREform **BEFORE commencing your research**. Please apply for ethical approval using the MOREform (https://moreform.mdx.ac.uk/). Consult your supervisor for guidance. Also see *Middlesex Online Research Ethics (*MyLearning area*) and* *www.tiny.cc/mdx-ethics*

If you have answered 'No' to ALL of the items in the table, your application is Low Risk and you may NOT require ethical review and approval using the MOREform before commencing your research. Your research supervisor will confirm this below.

Student Signature: Mahie Date: 01/03/2025

To be completed by the supervisor:

Based on the details provided in the self-assesment form, I confirm that:	Insert Y or N
The study is Low Risk and *does not require* ethical review & approval using the MOREform	Y
The study *requires* ethical review and approval using the MOREform.	N

Supervisor Signature: CAN BASKENT Date: March 1, 2025