A user level security framework for IoT in the smart home

Manju Mohan Pillai

orcid.org/0000-0003-3448-048X

Thesis accepted in fulfilment of the requirements for the degree Doctor of Philosophy in Engineering with Computer Engineering at the North-West University

Promoter:	Prof. ASJ Helberg
Co-Promoter:	Prof. MJ Grobler
Graduation:	June 2023
Student number:	22065903

Declaration

I hereby declare that this thesis is a presentation of my original research work, conducted under the supervision of Prof. ASJ Helberg and Prof. MJ Grobler. Whenever contributions of others are involved, every effort has been made to indicate this clearly, with due reference to the literature. No part of this research has been submitted in the past or is being submitted, for a degree or examination at any other university.

November 2022

Language Editor's Declaration

Language Matters Pty Ltd
info@languagematters.co.za
082 920 2991
www.languagematters.co.za

Language editing – Translation – Transcription – Simultaneous interpreting

[Company E-mail]

156 O R Tambo Street

Miederpark

Potchefstroom

2531

This document certifies that the manuscript/title listed below has been edited, within reasonable, ethical and professional limits, for syntax, grammar, spelling, punctuation and specific stylistic requirements of the English language by one or more qualified language practitioner(s) at Language Matters. The editor's revisions and comments serve as recommendations; the overall quality of the final manuscript's contents remains the responsibility of the client/author. The language editor does not accept responsibility for any changes made to the manuscript after the issuing of this declaration.

Manuscript title: A user level security framework for IoT in the smart home

Author(s): Manju Mohan Pillai

Date Issued: 22 November 2022

Issued by: BGS Language Matters and Media Services

Acknowledgement

I do not know how to begin to thank my Guru, Prof. ASJ Helberg who not only served as my supervisor, but supported, encouraged, advised, and guided me throughout this academic program. I do not think this thesis would have been completed without his guidance or support and I am forever grateful to him.

I extend my sincere gratitude to my co supervisor Prof. MJ Grobler for her valuable inputs.

I extend my sincere thanks to 'Language Matters' and especially Ms. Simone Barroso for proofreading this thesis.

I am thankful and extend my sincere gratitude to Dr. Kishor Krishnan Nair, who has provided valuable support in the completion of this study.

I am forever indebted in life to my mother Pushpalatha Pillai and my father N.C.M Pillai for making me who I am and for their continuous prayers. It was my father's wish that I continue to do my PhD and it is to him I dedicate this research.

I also thank my motivations in life, my daughters Keerthana, Kritha and Krisha and express gratitude for all their prayers and encouragement. If I can do this much, I am sure you can even do better.

The Almighty God has constantly guided me and carried me forward in life, beyond where I see myself. For me, nothing is possible without You.

Abstract

Internet of Things (IoT) devices and applications are growing in popularity for smart home use cases. Although experts have reported on the importance of implementing security measures in smart home devices for several years, studies reveal that most devices released on the market have multiple security vulnerabilities and, in many cases, no implemented security mechanisms. These vulnerabilities of smart home networks are mostly attributed to users' ignorance of security. Many users are unaware and lack the technical skills or knowledge about how their devices operate in their smart home environment. Existing research has raised the fact that users should be involved in mitigating security issues and protecting their own smart home devices. This research introduces a design that helps with user involvement and helps users protect their devices using simple configurations that can alert users of intrusions, thus helping to bring user awareness of their own smart home environment. These configurations create device interaction rules that are added to an existing network intrusion detection system (NIDS) in the smart home network. The research further discusses the generation of rules through user configuration that can detect intrusions. The design can be implemented in any internal smart home network irrespective of the number of users or device profiles within the home environment. Another advantage to such rule generation for smart home network use is that every smart home environment may not have the same rules generated through user configurations, as the rules are totally dependent on the user configurations. In addition to this, an existing attack signature is also introduced to detect specific attacks. These rules generate alarms that alert the user if unwanted interaction takes place between their devices or from an external network, in this way making users aware of the security breaches in their smart home network.

Publications based on this work

Some of the results obtained from this study and presented in this thesis have been published in conference proceedings:

- A paper titled " Improving Security in Smart Home Networks through user-defined device interaction rules," for IEEE Africon 2021 [136].

These publications were part of this study and were generated during registration for the PhD degree from 2016 to 2022. This work has not been used in whole or in part for any other qualification here or elsewhere.

Table of Contents

Figures

Tables

Acronyms and Abbreviations

Adaptive network topology (ANT)

Analytical and computing engines (ACE)

Anonymous Secure Framework (ASF)

Artificial Intelligence (AI)

Cloud Infrastructure (CI)

Collaborative intrusion detection framework (COLIDE)

Collaborative, seamless and adaptive sentinel for the internet of things (COSMOS)

Confidentiality, integrity, and availability (CIA)

Device capability exposure (DCE)

Dynamic host configuration protocol (DHCP)

Distributed denial of service (DDoS)

Extreme learning machine and artificial immune system (AIS-ELM)

Graphical user interface (GUI)

Host-based intrusion detection system (HIDS)

Hybrid broadcast-broadband television standard (HbbTV)

Information communication technology (ICT)

Information security risk analysis (ISRA)

Integrated development environment (IDE)

International organization for standardization (ISO)

International telecommunication union (ITU)

Internet of things (IoT)

Internet service provider (ISP)

Intrusion detection system (IDS)

Media access control (MAC)

Network infrastructure (NI)

Network intrusion detection system (NIDS)

National institute of standards and technology (NIST)

Radio frequency identification (RFID)

Raw information and processed data stores (RI-PD-S)

RFID sensor network (RSN)

Security information and event management (SIEM)

Self-Learning and adaptive smart home framework by integrating IOT with big data analytics (SLASH)

Short message service (SMS)

Solid state drive (SSD)

Structured system analysis and design methodology (SSADM)

Things with networked sensors and actuators (TNSA)

Transmission control protocol (TCP)

United Nations (UN)

User datagram protocol (UDP)

Wireless sensor network (WSN)

1

Introduction

1.1 Introduction

The Internet has become a fundamental technology in daily life. From shopping to paying bills, performing financial transactions, social networks, and research, the Internet has become the first stop for finding all the answers. The statistics of the International Telecommunication Union (ITU) indicate that internet is used by 4.1 billion people, which is 53.6% of the global population [1]. In 2020, the percentage increased by approximately 4%, making it to 59% by July 2020 [2]. With its vast demand, there have been many opportunities for criminals to access information legitimately. Many security measures have also been adopted as well. *The Internet of Things* (IoT) has become a vibrant and promising technology to develop powerful smart systems. [5]

IoT is the development of the Internet, where everyday computing devices or interconnected machines connect and communicate with each other by using electronics, software, sensors and can send and receive data without direct human-to-human or human-to-machine interaction. The Global Standards Initiative on IoT defines IoT as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) *things* based on existing and evolving interoperable information and communication technologies” [9]. Various application domains such as energy efficiency, Green IT, and logistics are starting to benefit from IoT [4].

Over the last few years, the immense growth of IoT has transformed the way we live and interact with each other and with numerous types of devices and systems which form part of the information communication technology (ICT) infrastructure [112]. IoT

has an important impact on numerous application domains including health care, smart home, agriculture, transportation, energy, manufacturing, and many others [112]. This research focuses on smart homes.

A smart home environment is an environment in which devices can connect to the Internet, analyse user data, and make autonomous decisions [24]. A smart home environment has one or more smart home devices, including sensing devices, smart appliances, health devices, and smart furniture. These devices usually come from different vendors that support various types of communication technologies.

Smart homes can obtain and apply knowledge about the users and their surroundings to provide more humanised home services and to perform daily tasks more easily than before [110]. The use of smart home devices can instil the feeling of both security and ease of use of these devices [111]. Thus, smart homes are a significant part of IoT that "[enable] a smart home user to have smart devices, multiple sensors and appliances that can be remotely controlled and operated through smartphone applications or personal computers"

1.1.1 IoT devices

IoT devices refers to physical or virtual objects. The ITU defines a *thing* as 'an object of the physical world (physical *things*) or the information world (virtual things), which is capable of being identified and integrated into communication networks' [9]. Virtual *things* connect to a gateway to communicate to the external world or to external servers, which may be a cloud or services such as applications of service providers that develop these *thing*s. Devices or *things* need to communicate and transmit data to other *thing*s or their application. Therefore, these *thing*s are linked to cloud services or external servers using predefined authentication mechanisms provided by the service providers. In this way, the *thing* is authenticated and authorised to communicate with its service provider according to its service capabilities. The ITU defines a device as a host that has the device capability exposure (DCE), provides underlying hardware/software support to implement the functionalities of DCE, and can connect to external IoT devices [11].

Some service providers may transfer the data received from a *thing* to a server or to a cloud, and then perform data analytics and even provide artificial intelligence (AI)

capabilities. Other services, such as weather information, may also be provided. Therefore, service portals, application management, risk and security management, and information management can also be dealt with at this stage. The data received may be transferred or transformed using the same principles as mentioned above to an enterprise architecture of storage and IoT services. Big corporations offer a wide range of connectivity and data aggregation and data transformation in the form of single products, software, hardware, infrastructure, connectivity, and analytics to interconnect many devices and thereby make it possible to communicate with each other. The architectures also mention aspects of security elements. The next section discusses the security environment and risks associated with IoT.

1.1.2 IoT Security Environment and risks

Cyber security relates to the protection of data and its systems. Any technological advancement such as IoT, cloud computing, smart phones and how society utilises these through the Internet adapts how these systems and data are protected [121].

All well-known IoT service providers provide security at the connectivity level to store data for data transport and, at the administrator level, secure the IoT architectures that are in place. The security features provided, at various points of the architecture, are the same features that currently exist when connecting over the Internet. Firewalls or authentication mechanisms that are present as part of the normal network security are applicable to IoT devices as well. There are only generalised security features that provide security to IoT devices only such as authorised software, firewalls to external network when connecting to the external network, and this is seen as a loophole. Many smart devices available in the market today, do not comply to security practices and standards that generally one would find on personal computers, and security is not the primary concern for various device manufacturers [100, 23, 139].

Much research discusses standardising IoT devices, however the technology is still developing. A major concern is educating users about potential compromises of their personal devices in the event of an attack as ‘security first’ is an idea that has not been efficiently applied to IoT. Even IoT devices developed by most large technology companies such as Amazon, Google and Apple are not secure in reality [111].

The ITU also identified security threats that can affect safety and security capabilities of the IoT [10]. Researchers have shown that there are several cases where smart *things* were compromised [23, 24, 25, 26]. The main approach for attack is to compromise one device or *thing* in the IoT network and perform fraudulent actions towards another connected *thing*, imitating the real one. Intruders have used 'smart' household appliances to launch IoT-based cyberattacks where everyday household *things* such as home network routers, televisions, and refrigerators have been compromised. Once compromised, it was used as a platform to send thousands of phishing and spam emails [24].

There are several reasons why IoT systems are at risk [5, 10, 15, 16, 19]. Firstly, they do not have well-defined boundaries. Secondly, they are highly dynamic and mobile as they can continuously change their locations and operating patterns. All IoT systems are different in terms of communication mediums, protocols, platforms, and devices. IoT systems, or fragments thereof, may be physically vulnerable and/or controlled by different parties [20, 23]. Conventional security countermeasures such as data encryption, user authentication, and security network tools (firewalls, network address translations (NATs)) act as the first line of defence against external threats. However, intruders or unauthorised users can compromise these countermeasures and access IoT devices [25].

Security concerns were raised, as early as 2006, for exposing smart home and its devices to the internet [18]. Most manufacturers do not create security and privacy solutions by design. This leads to a lack of security measures on IoT and smart home devices. As of 2021, the low-end user penetration of the smart-home market reflects that user do not favour using home IoT and smart-home solutions due to the number of security compromises that have been raised by other smart home users. Privacy concerns are an important factor that hampers the smart-home adoption according to research [116]. Smart home devices can monitor the status of their users, detecting when they are inside the house, when they leave or what activities they are performing [117].

The ITU also identified the need for home automation solutions as a need for smart city projects initiated by governments or integrated townships. This is because a smart home can become a part of the ecosystem comprising of (but not limited to) numerous city assets such as utilities, healthcare, transportation, waste management, law enforcement,

etc. To become a part of the larger ecosystem, the smart home can help the entire ecosystem integrate more efficiently and seamlessly; therefore, smart home/home automation systems should be viewed as building blocks to build smart cities as well [9]. Hence, the security vulnerabilities in smart homes can extend to smart cities as well. Therefore, implementing security in a smart home could also help smart cities. Smart home devices are designed to fulfil multiple functionalities and can connect directly to the Internet, controlled with an app, pass data back and forth, connect to the Internet through a router, connect to other devices within a network, and, possibly in the future, connect to external devices on the Internet [24].

Many vulnerabilities and security attacks have threatened and infiltrated the sphere IoT devices and networks which are increasing and evolving as IoT advances [14]; the results from Williams *et al.* showed that 12.92% of consumer devices have vulnerabilities and some devices have multiple vulnerabilities [14].

A study [18] showed that 40.3% of smart homes worldwide had five or more devices connected to the internet. Out of this, 40.8% of homes had at least one vulnerable device that risked the safety of the entire home. Studies also revealed that security of televisions, webcams, home printers, smart lightbulbs, smart power switches, smart plugs, and smoke-alarms could be easily compromised. The reported attacks on Google's nest devices put many families – including children – at risk due to security vulnerabilities and hackers controlling smart homes, exposing a major flaw in smart home devices, and thus calling for user security [7].

For example, in one incident in 2019, a couple's smart home was breached, and hackers took control of their smart home by compromising the households' connected devices. The attacker spoke to the couple through a kitchen camera while playing upsetting music from the video system. The attackers also took control of the thermostat and adjusted the room temperature to 90 degrees Fahrenheit. There have also been many reports of security flaws in smart bulbs where the bulbs were hacked through commands that were sent through the bulbs' infrared invisible light to hack other connected IoT devices on the home network. A smartphone's vulnerability is that it can be used to launch an acoustic side-channel attack [113]. Hackers have also used the integrated cameras and microphones in Smart TVs to change channels or volume control and to spy on the users' daily routine and conversations [113]. Identity and bank details can be stolen

through a coffee machine when users shop using their cards [113]. Many other researchers also noted that various smart home devices have numerous security vulnerabilities. These have already been analysed and can be found in existing vulnerability databases [13]. Another study [9] found many risks associated with users in which smart cameras disseminated sensitive data that include geographical locations and even combinations of usernames and passwords.

Smart homes, compared to other IoT applications such as smart cities, smart buildings, and smart retail, are directly associated with users and are smaller networks that can connect to the outside network using a hub or gateway [112]. Smart home networks are also different from each other. These security risks can do more harm to a user than the actual benefits from using the IoT devices. Users are unaware when their devices may operate without being triggered by them. They are also unaware of which other devices are connected to their devices, what information (possibly personal information) is transmitted from their devices, where this information is stored, who has access to the information transmitted, who has information on the events that are triggered by their devices, and what can happen if these devices are compromised [26, 14].

The ITU gave a contextual description of home automation and further described the interaction of users or homeowners. This highlighted two points of interaction. The first was in use cases such as triggering a device by switching it on, and the second was when the users would be alerted if an unwanted event such as fire or theft happened. [9]

When IoT smart home devices need to be configured, the major challenge is the lack of configuration tools and interfaces, which offer minimal education to the user. These configuration tools act as a safeguard measure for the users. Furthermore, users are unaware of the technology that smart devices are built on, hence users prioritise the convenience that a device offers over their security. To do this, user interactions need to be understood in a smart home environment. A detailed discussion related to existing research and context is provided in Chapter 2 and Chapter 3.

1.2 Research motivation

With the growth in IoT, wireless communication has focused on how to effectively enable IoT communication between devices [39], which is applicable also to smart home

devices. However, users may not be aware that this sort of connectivity puts them at risk of privacy and security breaches unless technological companies or third parties that provide these services mange data ethically [111]. The value of such exchanged information in smart homes is very high and may be confidential to its users. These smart home devices become attractive targets for intrusions that aim to gain access to sensitive information, violating confidentiality, integrity and availability of such users' data [112].

Smart home devices face the risks associated with transferring and communicating data. For example, the organisation of multiple points of data can quickly become personal information as events are analysed in the context of time, location, and recurrence. The consistent purchase of different types of food may disclose religion or ongoing health concerns, for example, gluten-free products may indicate the lifestyle of users [40]. The regular recurrence of events triggered by an application may indicate a person's routines.

The above vulnerabilities have risen with the increase in IoT, and smart home devices driven by the conjunction of market forces and parallel innovation of technologies. Products have changed from mere physical products to complex systems combining sensors, processors, software, and digital user interfaces that are now connected to the Internet and each other [41]. This complexity, especially in a smart home environment with multiple devices from different manufacturers, makes implementing a single security measure challenging.

The configuration of each capability for a specific device could be different, time consuming, and complicated [8]. Hence, users must be aware and take security measures so that their privacy and security are not compromised.

1.3 Research problem

In smart home environments, it is difficult to implement security mechanisms because: (1) It is a heterogeneous ecosystem that integrates numerous types of devices, technologies and services; (2) most of these devices are intended to perform a certain functionality. Hence, security support is limited because of their weak capacities (battery, CPU etc.); and (3) many devices or systems within these devices have remote

infrastructures (analytics, cloud storage, or remote access to the devices) to offer their services [119].

With the technological advancements such as IoT and Smart homes, more criminals target users using the vulnerable point in the current information system. The intruder will combine some social engineering methods and use personal information transmitted by these devices to attack people, to seek their own interests [122]. Hence cyber security awareness which relates to how much users are aware of risks associated in the systems they use and how they can mitigate them in the event of an attack plays an important role in securing these systems.

Privacy and security concerns including access control are the most significant among factors in the IoT context due to the massive volume of personal and sensitive data they collect. The privacy concerns and data security involving IoT devices and smart homes need attention from multiple stakeholders such as manufacturers, security professionals, government agencies, and the users themselves [115]. Hence there is substantial evidence that information privacy is a major concern between a user and an online entity. Despite this, few efforts have been made to explore the linkages between the drivers/inhibitors of smart home devices and privacy concerns. Hence, current privacy literatures are not only partial towards the information privacy perspective, but also lack in developing a complete theoretical framework that will recognise and study the various backgrounds of privacy concerns [116].

In a smart home, many devices are interconnected, and activities are automated. The technology is deeply integrated into the users' daily routine. In such homes, physical privacy may be compromised either due to recording of various personal activities, continuous surveillance or from intrusions such as invasion and spying on private properties. The probability of physical privacy infringement has further increased greatly with the arrival of advanced IoT technologies, which are vulnerable even without a physical intrusion. Existing research has recognised another negative aspect of home automation on the users' self-perception or peace of mind. Existing research also indicates that much of the public fear's automation, which can be a great psychological barrier to adapting the automated technology. With the arrival of new attacks and vulnerabilities, automated monitoring is vital to identify the risks occurring from such threats or potential configuration or manufacturing failures [116].

All of user's connected devices can be affected due to the nature of smart devices and IoT and existing security vulnerabilities in the network. Data processing is another vulnerability that can affect IoT devices [3]. Users may not be aware of these security vulnerabilities [13] and thus not be aware of unauthorised access or how to prevent it. This is a great shortcoming, as unauthorised access to the smart home system is one of the most destructive actions and can cause several home privacies issues. Access control is one of the best solutions for managing this threat, and it has been used to protect smart homes and other IoT domains for many years [102, 112].

Many research papers concluded that users are at threat due to privacy and security concerns. They include Bugeja *et al.* [75], which presented a comprehensive analysis of potential intrusions and vulnerabilities to the security and privacy of users using a smart home device and specifically devices, communications, and service. The authors provide a solution by defining a security architecture framework and then raise the need for additional research focused on four aspects of connected smart homes. These are (a) identity management, (b) control of information flow, (c) risk assessment methods, and (d) management methods of security. Jacobsson *et al.* [76] and Wilde *et al.* [72], evaluated the vulnerabilities and threats of a smart home through a common risk analysis method, ISRA (Information Security Risk Analysis), and discussed the consequences for user privacy for specific scenarios. Pardeep *et al.* [77] also proposed the Anonymous Secure Framework (ASF) for the smart home, based on four requirements, specifically (i) anonymity and unlink ability, (ii) authentication and integrity, (iii) low communication cost and computation complexity, and (iv) security safeguarding. Chavis *et al.* [120] in their research proposed a design using voice assistants to provide the security state of the IoT network to users. This design uses a combination of machine-learning-enriched devices and dynamic visualisation of IoT networks for the voice assistant to communicate status and issues to the user. However further details of the data or devices that was learned included, and a thorough solution on how it would help the user was not detailed in the paper. These papers also identified that users are at risk when using smart devices.

Users do not have the authority or indication of the data that is passed through the different interconnected systems and of the various infrastructure that is used in IoT systems. This ignorance of users on how smart homes work and transmit data can cause

more damage to the user than actual benefits offered by IoT devices. In the case of smart home devices, the above-mentioned problems are increasing the risks of homes to criminals [16,26]. In essence, users may not have the skills, or the time needed to monitor their own smart home network. They may also not be able to understand data from tools that are present to monitor and protect their smart home environment [120]. In addition, for nontechnical users, this is bothersome, especially as users do not know how to protect themselves from intruders. Also, cyber physical attacks can affect domestic life and a person's behaviour and psychological state in their own home [92].

This lack of user awareness calls for a redesign of smart home configuration tools and interfaces [22, 9]. Due to the development of threats, it is imperative to raise this security awareness among users and specifically among smart home users [27]. Considering this, the trust relationship between users and IoT devices is a major factor for IoT devices to flourish. Several authors argued that users are responsible for safeguarding their own devices and not performing appropriate IoT devices installations in smart home environments can make their information vulnerable [45, 113, 115, 111].

Security and privacy are a major concern in smart homes to heterogeneous environment. Users are not aware of all the risks associated and the research community have analysed the risks users can face and has advised that users should be involved in protecting their smart home devices and users should be aware of the security of their own smart home devices as a need, considering that not all users are necessarily technologically literate or inclined. This means that trust is needed to increase the adoption of smart home IoT, and users must be educated on their responsibility around appropriate installations and safeguards.

1.4 Research goal

With the real-life scenarios that have occurred, users were not aware of the intrusive connections that happened within their homes except when the intruders started controlling their homes [7, 8, 14, 113]. The goal of this research is to address the crucial gap of how to involve users in smart home security as mentioned in various literature by involving users (technical or non-technical) and showing them how to identify their smart home devices in the smart home environment. The research aims to increase user involvement by creating user configurations that can alert them of security breaches

happening in their smart homes. This should be achieved through user configurations and thus make users aware of security intrusions happening in their smart homes through alerts. The wide differences in devices, communication protocols, technologies used within the smart home environment should not affect what the user will have to configure. Given that users are both technically and non-technically capable and that smart homes are a heterogeneous environment, a mitigation strategy that can be applied when an intrusion happens is not in the scope of this research.

The research goal is achieved through the following specific goals.

- Develop a design that allows users to detect intrusions as they occur within their smart homes based on user configuration.
    - The configuration proposed should work for every smart home environment irrespective of the number of devices or number of users within the smart home.
    - Users should be involved in configuring parameters that can alert them about intrusions on their devices. These configurations and alerts should make users aware of the security of their smart home.
    - The configurations that a user inputs should be unique to how the user wants the smart home device to function.
- Adapt the functionality of intrusion detection systems to configure, alert and thus make users aware:
    - Users are alerted about intrusions through the interface.

The goals are achieved by answering some key questions as follows.

1.4.1 *What is the general architecture of IoT and that of the smart home?*

This research question aims to offer an understanding of the existing general architecture and the smart home and of how to develop the new design above.

1.4.2 *What is the existing user-level security in the perception layer and the application layer in the current IoT architecture?*

This research question is addressed through a comprehensive study of the user-level vulnerabilities and existing security measures in the application layer and the perception layer of different IoT smart home architectures.

1.4.3 *What methodology or technology can be used to improve security and privacy?*

This will evaluate existing research that has been done to understand existing research solutions to develop a solution that can be used for users to configure security so that they can be alerted when their devices are not functioning normally.

1.4.4 *What are some of the existing researches that provides user security and how does the solution proposed at the user level differ?*

This section will discuss any existing solutions that validate and verify how the proposed solution differs from existing solutions.

1.5 Research methodology

This research uses a general IoT project methodology [108, 109] combined with a quantitative approach and prototyping methodology to fulfil the research goal.

The IoT project methodology involves the structure of an IoT smart home project. There are three steps involved in this methodology. They are (1) requirements analysis, (2) preparation of development, and (3) IoT software and hardware requirements. How these would be applied are explained in the sections that follow.

Quantitative research is defined as the systematic empirical investigation of social phenomena via mathematical, computational, or statistical techniques to develop and use mathematical models, theories, and/or hypotheses about a phenomenon. It is carried out using scientific methods such as the generation of theories, models, and hypotheses, collection of empirical data, and data modelling and analysis [28]. Quantitative research has the following steps: (1) identify a problem, (2) review the literature, (3) specify a purpose, (4) collect data, (5) analyse and interpret data and (6) report and evaluate [29].

This research starts by reviewing existing literature studying IoT and the importance and usability of IoT applications and specifically smart homes. The research then continues by reviewing literature by studying the IoT architecture and that of smart homes. The existing literature is studied to understand and identify methods or technologies that can be used to solve the research problem. This then evolves to identify the design to meet the research goal. The design is developed using the structured system

analysis and design methodology (SSADM) [90] as well as the requirements analysis from the IoT project methodology. Once the design is developed, a prototype is developed using the development preparation and hardware and software requirements of the IoT project methodology leading to the development of the prototype using the prototyping methodology.

The prototype is simulated to follow the working design and will be tested and measured against the available standards. Data collected from the prototype is analysed, interpreted through testing, and results are verified and validated in detail against the design. These results are then evaluated and summarised.

1.6 Thesis layout

Chapter 1 introduces the research, explains and motivates the research problem, identifies the research goal, and explains the research methodology for the research

Chapter 2 provides a background to IoT, and its applications motivate why smart home devices were selected for research. It then continues by providing a thorough investigation on IoT architecture and smart home architecture. This chapter also describes security, security vulnerabilities, and why security is required in IoT.

Chapter 3 describes existing security models in IoT and identifies any similarities or differences between existing and the research proposed.

Chapter 4 proposes the design and conducts an in-depth analysis of the proposed design to determine if it can indeed address the research problem. Individual entities in the system are designed using structured system analysis and design methodology.

Chapter 5 models the functional prototype. The design is discussed in detail, and a prototype is provided to demonstrate the proof of concept.

Chapter 6 validates and verifies the prototype against the functionalities and intrusion detection rate on known and unknown intrusions. It evaluates the prototype with existing research and available applications. The results are also analysed and noted.

Chapter 7 concludes the thesis by summarising the importance of this study. It describes the significance of this research and its specific contributions. The applications of this research, its limitations, and the scope for improvement are also provided in this chapter.

2
Internet of Things (IoT)

Most of the major companies in the IT industry have invested in developing IoT products, and every day there is a new company that is introducing a new IoT product or service. With the growth in IoT and smart home devices, it is vital to understand what IoT is, provide background to IoT, discuss the architecture and framework of IoT and smart homes and its applications, and understand security and flaws.

2.1 Background to IoT

The concept of IoT has been present for years. The first Internet appliance was developed in 1980 at Carnegie Melon University; it was a Coke machine [5] that could connect to the Internet and allow developers to check the status of the machine and interpret whether a cold drink is available [5].

The actual concept of IoT was not conceived until 1999, although it has been in development for decades. The term IoT was first introduced by Auto-ID Labs in 1999. It was introduced for radio frequency identification (RFID) devices by Kevin Ashton [28]. Kevin Ashton first keyed the term 'Internet of Things' in a presentation he made to Procter & Gamble[1] in 1999. In the same year, Neil Gershenfeld from MIT Media

[1] **Procter & Gamble:** also known as P&G, is an American multinational consumer goods company headquartered in downtown Cincinnati, Ohio, United States, founded by William Procter and James Gamble, both from the United Kingdom.

Labs[2] spoke about *things* similar to IoT; and LG [3] Electronics also announced its first smart refrigerator plans.

In 2003-2004, popular publications such as 'The Guardian' and 'Scientific American' mentioned IoT. In 2005, IoT reached a new recognition level when the International Telecommunications Union (ITU) of the United Nations (UN) published its first report on IoT [29].

Over the years, IoT has evolved tremendously and is still a developing trend for both academia and industry [30]. The number of companies that use the IoT is growing exponentially. IoT has grown from 12% in 2013 to 29% in 2017 and 34% in 2019. Organisations that have invested in IoT have grown considerably over the years. There were altogether at least 10,000 connected devices and shared devices have doubled with more than 100,000 from 3% to 6%. By 2020, more than 65% of companies will adopt IoT products [31]. With the increasing complexity of IoT devices, the number of devices used in attacks are also increasing. Around 31 billion *things* are connected currently, and it is projected that this number will rise to 75 billion by 2025. Majority of these devices used by private consumers are smart home devices [123].

Every day a new company declares some IoT-enabled product. The tools and information available to secure smart home security and protect privacy has been criticised and certain issued have emerged in the field [34]. Some researchers believe that the value of the smart home devices market will reach 174 billion USD by 2025 [35].

A survey commissioned by Intel Corporation and conducted by TNS[4] also reveals that we are headed for smart home growth. Nearly 68% of Americans are confident that smart homes will be as common as smartphones in 10 years. Business intelligence from the industry echoes consumer feelings and predicts that connected home devices will

[2] **MIT Media Labs**: The MIT Media Lab is an interdisciplinary research laboratory at the Massachusetts Institute of Technology devoted to projects at the convergence of technology, multimedia, sciences, art and design.

[3] **LG:** LG Corporation formerly Lucky-GoldStar is a South Korean multinational corporation. It is the fourth-largest chaebol in South Korea.

[4] TNS: Kantar TNS (formerly known as Taylor Nelson Sofres) is a market research and market information group. Formerly listed on the London Stock Exchange and a constituent of the FTSE 250 Index, the firm was acquired by WPP Group in October 2008 for £1.6 billion.

grow at a compound annual rate of 67% in the next five years [36]. The next section discusses the IoT applications.

2.2 IoT Applications

Practical applications of IoT technology can be found in many industries today. ITU has suggested that IoT will link world objects in both an intelligent and a sensory manner. The IoT vision enhances the integration between 'anytime', 'anyplace' for anyone and 'anytime', 'anyplace' for anything. IoT has been applied in a variety of diverse environments, including logistics, asset tracking, transport, and smart environments (homes, buildings, infrastructure), energy, defence, and agriculture. In principle, the IoT can significantly have an impact in all aspects of society [6, 7, 112]. Furthermore, it creates enormous opportunities for companies to develop new services and products.

Recently, South Africa has seen a tremendous rise in investment in IoT. The South African IoT market is estimated to reach more than 2 billion rand (ZAR) by 2020 and is expected to transform all sectors' as more connected devices are emerging within these applications, as Vodafone suggests in Figure 2.1.

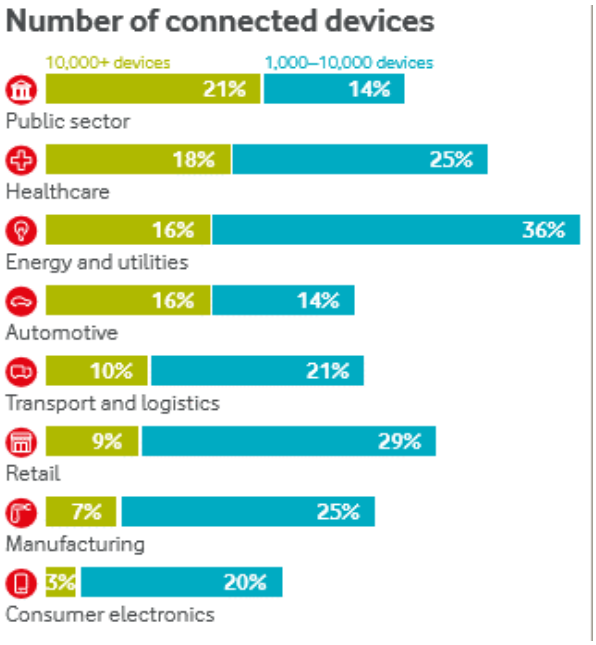


Figure 2.1: Number of connected devices according to Vodafone research [31]

Eighty-four percent (84%) of IoT companies have seen an increase in the use of IoT solutions in the last year, 12% of IoT invested corporations have at least 10,000

connected devices, and the total share with more than 50,000 connected devices has doubled from 3% to 6% [31].

In a survey from an IoT-I project in 2010, 65 IoT application sections were identified, which were grouped into 14 domains. These domains are transportation, smart city, smart home, agriculture, lifestyle, smart factory, retail, supply chain, health care, emergency, user interaction, environment and culture, energy and tourism [30, 112]. Asghar *et al.* [32] in their paper classifies IoT applications into six domains, smart home and smart building automation, healthcare, mobile communication, smart business, enterprise and utilities [32]. Many academic journals have named and categorised applications differently. HP classified IoT applications as smart home, wearables, connected cars, smart cities, smart retail, precision agriculture, building management, healthcare, energy, and IoT in poultry and farming [33]. The ITU has also defined 12 vertical domains and can be found in [9].

Smart home products can save time, money and energy for homeowners, with 87% of homeowners saying that these devices have made their lives easier. As a result, smart home products will become standard household brands in the coming years [35]. Users must think twice before considering connecting a smart home IoT device.

To understand any IoT application, including smart home applications and the way it functions, it is important to understand the architecture of IoT and specifically that of smart homes. These are explained in the next section.

2.3 IoT building blocks

The IoT can be explained through its architecture, which varies depending on the application in which it is accepted. The basic premise of architecture is explained by the concept called the building blocks of IoT [5]. A general understanding of the basic components was analysed and is presented in Figure 2.2.

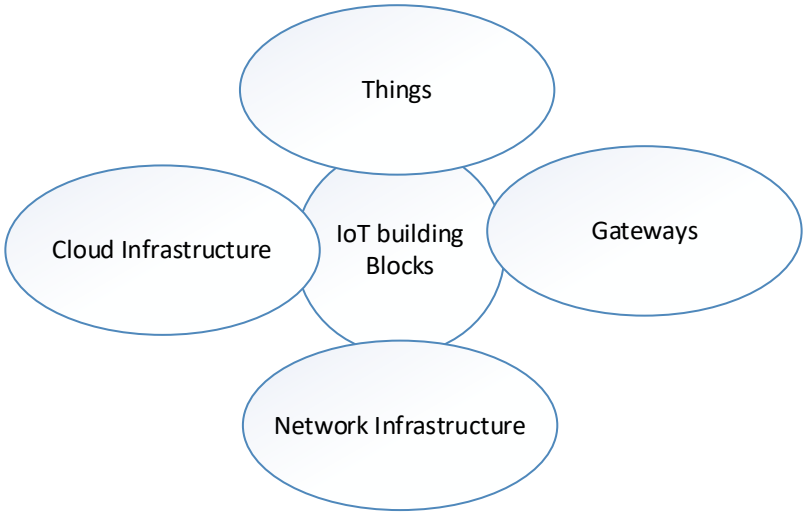


Figure 2.2: IoT Building Block Components

According to the above model, there are four main building blocks of IoT architecture, namely *things*, gateways, network infrastructure, and cloud infrastructure. *Things* could be physical or virtual, as explained earlier [33]. *Things* are devices in which information is sensed by sensors or actuators [5]. A physical *thing* may be represented via one or more virtual *things*, but a virtual *thing* may exist without any associated physical thing [33]. Gateways are used for connectivity purposes, and it is an integral part between the *things* and the network or cloud infrastructure. The network infrastructure (NI) is the network that allows a secure and smooth flow of information. The cloud infrastructure (CI) is the cloud where information storage and computing proficiencies take place.

The four building blocks are assembled into three components. The three main components of IoT include *things* with networked sensors and actuators (TNSAs), raw information and processed data stores (RI-PD-S), and analytical and computing engines (ACE). TNSAs collect information from objects or the *things*. Raw information and processed data stores (RI-PD-Ss) store the collected information in different forms: data, text, videos, images, models, etc. Analytical and computing engines (ACEs) help in the human-machine interactions and allow feedback as per the human requirements [5].

2.3.1 IoT framework

The IoT provides various solutions to most of the problems that the workforce is facing. The approach to achieve a solution is based on how components were integrated with communication devices with the best convergence of hardware and software

convergence. The software-defined hardware system processes the information, from where the analysis, storing and retrieving of data is done. Communication systems help to provide communication and allow protocols between objects or between *things* or each component of IoT [5, 35]. This will only happen when an effective IoT architecture layer is built. These architecture layers would differ depending upon the requirements and tasks to handle. Several architectures are presented in literature. While one divides architecture into layers based on characteristics, others have divided it into four layers or seven layers [5, 36, 123]. This section gives an overview of the generally agreed basic architecture of IoT which is the three-layered architecture, the architecture most used.

The three-layer framework consists of the application layer, the network layer and the perception layer as shown in the diagram below.

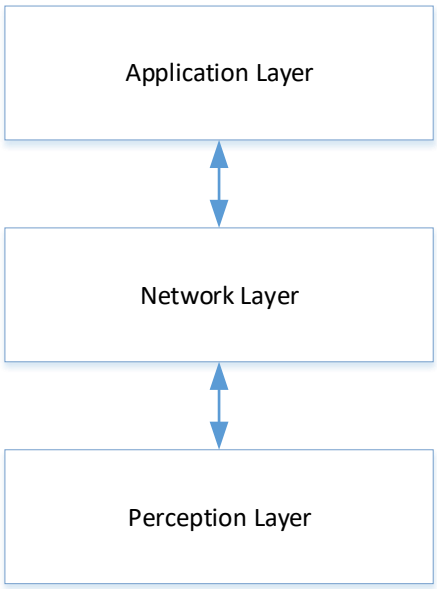


Figure 2.3: IoT Framework

The perception layer is the lowest layer and is also known as the control layer. The layer completes the collection of information of a person or *things* using perception tools such as sensors and transmitters. When all information is collected, the perception layer processes and packages the information and receives information from the network layer to control the devices [42]. The perception layer contains the *things* mentioned in the IoT building block.

The network layer is the middle layer in the framework that consists mainly of infrastructure components and is also known as the transmission layer, as it transfers the

information from the perception layer to the application layer [42]. This network layer constitutes the gateway or network in the general architecture.

The application layer is the top layer in the three-layer architecture. The application layer analyses the information transmitted from the perception layer through the network layer and recognises the IoT application. The application layer acts as the user interface between the IoT and various types of users or *things* [42]. The applications exist in the data processing application of the general architecture.

The building blocks of IoT and the general IoT architecture were explained above. An analysis of these is provided in the next section.

2.3.2 Evaluation of the IoT architecture, models, and framework

Devices or *things* connect to a gateway to communicate to the external world or to external servers, which may be a cloud or services such as applications of service providers including device makers. This makes up the perception layer. Devices or *things* that need to communicate and send data to service providers or other *things* are linked to the cloud services or external servers using predefined authentication mechanisms provided by the device makers or service providers. In this way, the thing is authenticated and authorised to communicate with its service provider according to its service capabilities. This communication, in which data is transferred and transformed happens over a network layer such as Ethernet, Wi-Fi, adaptive network technology (ANT), Bluetooth, ZigBee, or cellular networks such as 2G, 3G, or 4G. This communication happens through protocols or policies. Protocols may be used for infrastructure, data, and messaging, and different protocols are used for different layers of the network.

These protocols and policies used are dependent on the service providers and based on the service capabilities that they provide. Some service providers may transfer information to a server or cloud, which may perform data analytics and even provide the capabilities of artificial intelligence techniques. Other services such as weather information may also be provided. Therefore, service portals, application management, risk and security management, and information management may also be dealt with in this data transfer stage. The data received may be transferred or transformed using the

same principles as mentioned above to an enterprise architecture of storage and IoT services. Service providers offer a wide range of connectivity, data aggregation, and data transformation in the form of single products, software, hardware, infrastructure, connectivity, and analytics to interconnect many devices. This interconnection serves to enable them to communicate with each other, which constitutes the application layer. Some service providers may also provide security as a third-party service.

There are aspects of security elements, which are also mentioned in the architectures. In the three layers discussed in the previous section, it is visible that the perception layer comprises users and *things* in use. The network layer composes the different protocols and network infrastructure, which varies according to service providers. The application layer constitutes the data management and applications that control the data sent to users and things. These applications may also vary depending on service providers. The constitution and components in each layer also provide a self-explanation of where users are mostly involved, which is the perception layer and the application layer.

The smart home context and figure as explained by the ITU [10] is provided in the next section.

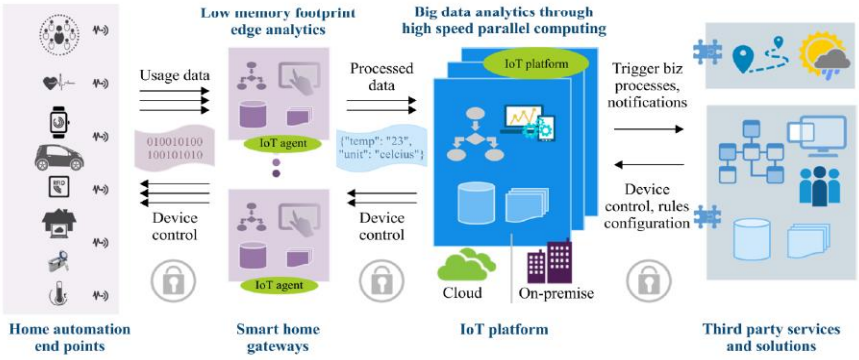


Figure 2.4: Home automation system [10]

In the home automation system diagram, the building blocks of the general IoT are followed, where the home automation endpoints are the *things*, smart home gateways are the gateway, the IoT platform is the network architecture, and third-party services and solutions are the cloud infrastructure that includes applications from service providers.

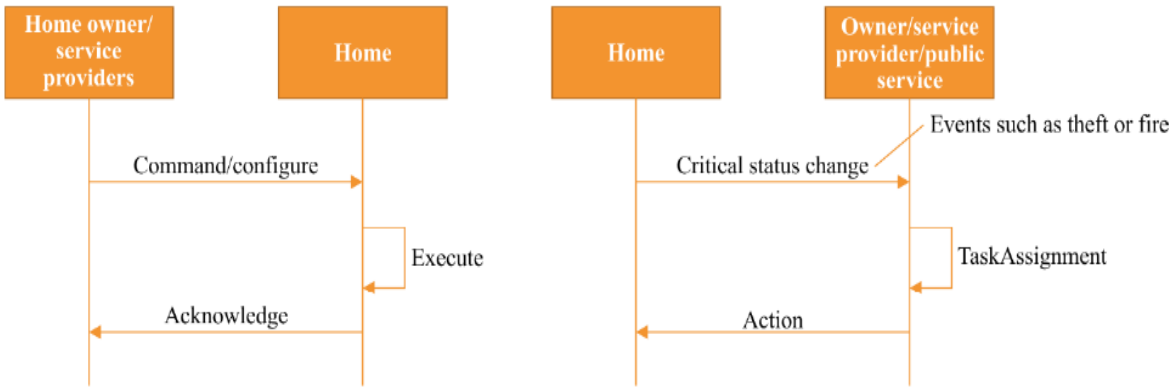


Figure 2.5: User Interaction in a Home automation system [10]

The users' or homeowners' role in this architecture is minimal, as shown in figure 2.4. Their role is to command or configure the devices in the home and alert the user of events.

The International Telecommunication Union (ITU) [10] explained the design of smart home automation design using the building blocks of general IoT. These building blocks of IoT are *things*, gateway, IoT infrastructure, and cloud infrastructure. In the smart home, the smart home devices are the *things*, a smart hub is a gateway that connects all the devices within the smart home, the IoT platform is the network architecture, and third-party services and solutions are the cloud infrastructure (which includes applications from service providers).

The architecture of a smart home consists of the way devices communicate with one another, how and where the information is stored and processed, and how the user interacts with the devices and vice versa [10,42,131]

In essence, smart home architecture can be shown as in Figure 2.6. This architecture can be split into two parts – the smart home internal architecture, which consists of the smart devices, smart hub and where users primarily interact, and the infrastructure outside the home, which is the external network. The smart home internal network part of the architecture is the focus of this research.

In the smart home architecture shown in Figure 2.6, the internet service provider (ISP) may take over the responsibility for secure service delivery. The service provider may involve an external company for a deep security analysis when the level of security

expertise level needed to detect advanced threats is beyond their competence. Users are unaware of who has access to their information, so it is important for users to have a ease in protecting their smart home devices.

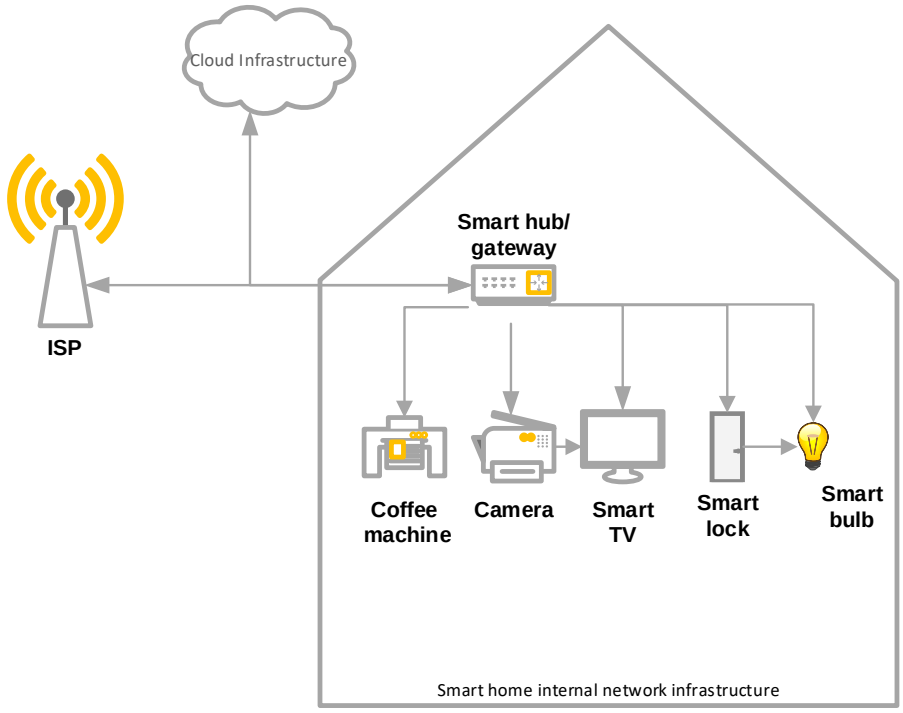


Figure 2.6: Smart home network

Security in the IoT is an important component that needs to be considered. The Vodafone IoT barometer [31] suggests that security is still a major concern, and of 10,000 connected devices, only 7% have considered security. Security and data privacy concerns are hence seen as the biggest barriers in IoT.

Smart home networks and specifically smart home internal network without protection can be considered an open environment and at high risk [22]. With the goal of a design to involve users, this research hence focuses on the smart home internal network.

The next section provides a brief overview of IoT security.

2.4 IoT security and privacy

IoT applications offer their users convenience, but if personal security is not considered, private data may be compromised. Therefore, security in the IoT cannot be ignored.

As IoT grows, traditional security issues have become severe and new security issues have arisen. The IoT contains many interconnected devices that communicate with each other to achieve specific goals. These devices have different technologies and connect to three different layers, which have been discussed in the framework section. The devices in the perception layer may have to perform the processes of communication, sensors, and identification. The application layer performs processing, visualisation, or interpretation of necessary data through different software. The network layer is used to connect the application layer and the hardware layer. Substantial work has been done to enable more effective IoT adoption in these layers to address privacy and security concerns [38] but ensuring privacy and security while enabling interoperability between multiple devices remains a challenge given the heterogeneous nature of devices [38, 112].

Zhang *et al.* mention that security problems are created by poor program designs of *things*, which can open a backdoor for malware installations. Then the networking environment of things is heterogeneous, meaning different communication mediums will face different security challenges [37].

One of the most significant aspects of improving the quality of IoT is the security of the IoT framework. Although a considerable amount of work has been done in the area of IoT architecture and IoT framework protocols, the issues around the security of *things* and the interaction between smart home IoT that could affect users when using a smart home IoT device have not been considered formally.

Figure 2.7 compiled using [43,45] defines the security architecture in IoT based on the framework layers. The security in all three layers ensures that the IoT device being used is secure. The application layer consists of IoT applications and an application support layer. This layer includes the security of service support platform security, cloud computing platform security, information development platform security in application support layer, and IoT application includes smart home security, smart grid security, and other application security [43].

The network layer is responsible for transforming information that comprises wireless and wired networks, network interfaces, communication channels, and intelligent processing. The network layer incorporates core system security, and access network

security, security of the local network. It also includes Wi-Fi security, ad-hoc network security, and 3G access network security, among others [43].

The perception layer includes RFID tags, sensor networks, smart cards, and wireless sensor network[5] (WSN) sensors, which ensure the worthiness and secrecy of data. The perception layer consists of RFID security[6], RSN (RFID sensor network) security[7], WSN security[8] to mention a few [43].

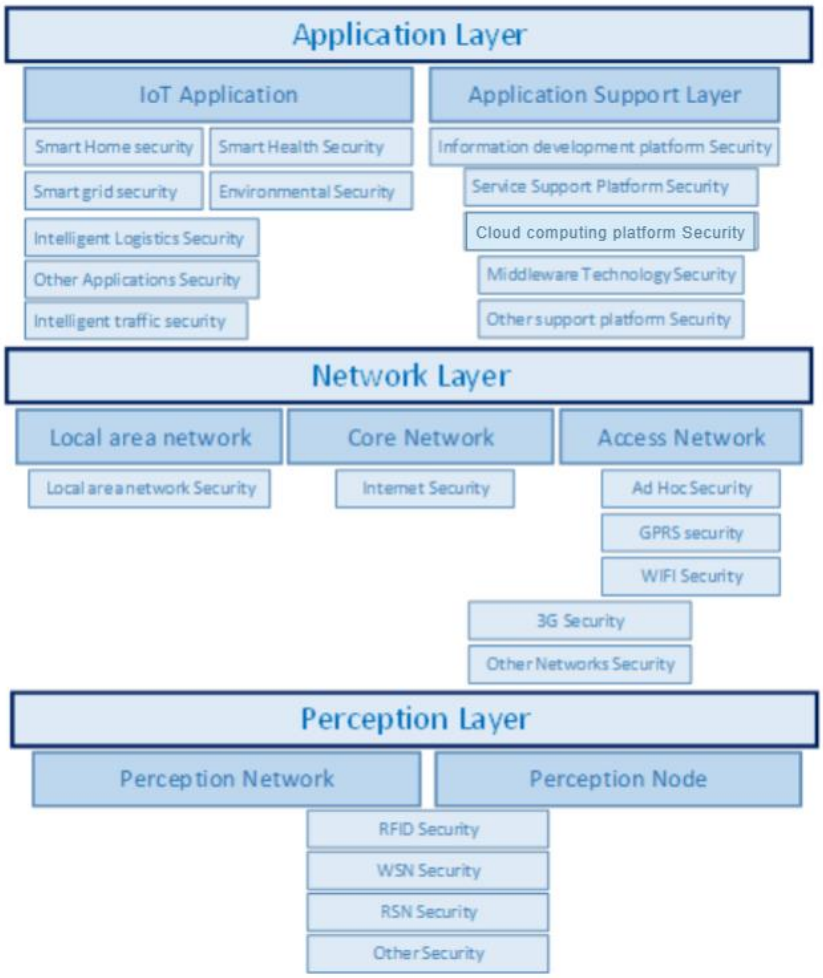


Figure 2.7: Security architecture

[5] Wireless Sensor Network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organising the collected data at a central location.

[6] RFID security: security problems related to no uniform international encoding standard for RFID tag, conflict collision, [RFID] privacy protection, trust management

[7] RSN security: (RFID sensor network) security: security problems of heterogeneous integration (integration of RFID and WSN)

[8] WSN security: cryptographic algorithms for WSN, key management in WSN, secure routing protocols for WSN, trust management of WSN nodes

Each network communication and IoT application has unique technology and unique requirements [43]. Hence, applying security at the network layer and at application level becomes difficult.

The next section explains the potential security threats at the perception layer and the application layer and specifically evaluates at the user level using the security and privacy controls.

2.4.1 Security in perception and application layer

The perception layer consists of sensors [43]. It collects, detects, processes, and transmits information with the help of sensors and actuators. The first issue in the perception layer is the strength of the wireless as signals are transmitted between sensor nodes using wireless technology. Second, the IoT nodes are operated in an external environment, which is vulnerable to tampering [47, 112]. The intruder can physically damage or control the device by easily gaining access [43]. In addition to these, these devices may also be susceptible to existing cyber-attacks [43]. Since devices in the perception layer exchange a large amount of secure and private data, they are susceptible to various attacks [46].

The diverse nature of network topologies in devices, sensors, and applications makes it difficult to provide security for each component in the perception layer. One of the major security goals of the IoT is to provide appropriate authentication mechanisms, a reliable connection, and confidentiality of the data to each device connected to the network. Hence, any threats to these in any network and particularly in a smart home network could have a harmful impact on its users. Therefore, security for the user could be provided in the perception layer by involving users.

The application layer supports different types of business services and assigns resources in the selection, processing, and production of data. This layer also filters the data. It includes service support platforms, cloud computing platforms and middleware. The major issues in this layer originate from the different applications used by different service platforms [43].

Most devices found in a smart home that were analysed were discovered to have serious security vulnerabilities [15, 93]. Many threats associated with these devices were also defined in [22, 94]. The following figure is a representation of IoT attacks based on the architecture layer and the IoT building blocks applicable to smart homes from [95].

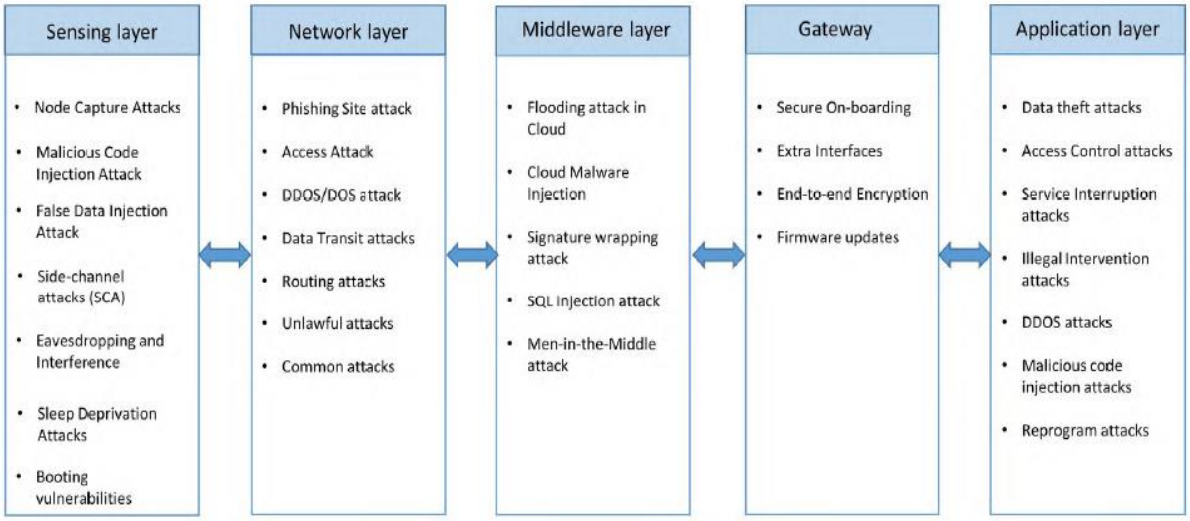


Figure 2.8: IoT attacks per layer

Many of these smart devices require users to disclose some personal information in exchange for advanced and more personalised services. This demands security and privacy in the design of IoT technologies and services. In previous years, consideration has been paid to the risks related to the use of simple IoT devices. Furthermore, certain security attacks against commercial IoT devices and particularly in smart homes have appeared in the media, contributing to raising public awareness of the security threats associated with the world of IoT [79].

The intruder can perform the attack on the IoT system by damaging or tampering with some device's physical vulnerability or a vulnerability in its network by using vulnerabilities in routing protocol and other network-related protocol, or from applications on the system, and could also have attacks from a malicious program, i.e., encryption attack. In smart home devices, this compromises the security and privacy of smart homeowners. Based on these vulnerabilities, attacks can be classified into four categories, as shown in the next figure [80].

<table>
<tr><th>Physical Attacks</th><th>Network Attacks</th><th>Software Attacks</th><th>Encryption Attacks</th></tr>
<tr><td>Node Tampering</td><td>Traffic Analysis Attacks</td><td rowspan="2">Virus and Worms</td><td>Side Chanel Attacks</td></tr>
<tr><td>RF Interference</td><td>RFID Spoofing</td><td rowspan="5">Cryptanalysis Attacks:
a) Ciphertext Only Attack
b) Known Plaintext Attack
c) Chosen Plaintext or Ciphertext Attack</td></tr>
<tr><td>Node Jamming</td><td>RFID Cloning</td><td rowspan="2">Spyware and Adware</td></tr>
<tr><td>Malicious Node Injection</td><td>RFID Unauthorised Access</td></tr>
<tr><td>Physical Damage</td><td>Sinkhole Attack</td><td rowspan="3">Trojan Horse</td></tr>
<tr><td>Social Engineering</td><td>Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Sleep Deprivation Attack</td><td rowspan="2">Denial of Service</td></tr>
<tr><td rowspan="2">Malicious scripts</td><td rowspan="3">Man In the Middle Attack</td></tr>
<tr><td rowspan="2">Malicious Code Injection on the Node</td><td rowspan="2">Routing Information Attacks</td></tr>
<tr><td>Sybil Attack</td><td>Denial of Service</td></tr>
</table>

Figure 2.9: IoT attacks

IoT framework solutions such as key administration and access control must also meet the security requirements of the device or service they provide [51]. Security demands cannot be accomplished in a single layer. For example, if an information security had been applied in the perception layer, it is easy for an intruder to get private data easily if the application layer is weak. Therefore, collaboration between various layers is needed [43].

There are technical and non-technical security measures that can be provided. Technical security measures include key agreement and authentication between various networks to avoid man-in-the-middle attacks and other similar attacks that are dependent on the public-key cryptosystem (PKI certificate), based on symmetric key cryptosystem and certification transfer technology [43].

The nontechnical security measure lets customers or users understand the importance of data security and how to use IoT administration effectively in order to avoid and reduce data leakage and compromise of data [43]. A design that meets this aim should involve users and make them more aware of the security of their smart home devices through alerts, considering both technical and not technical users can be considered as a nontechnical security measure.

A classification of countermeasures is represented in Table 2.1 [94].

Table 2.1: countermeasures per layer

IoT Layer	Counter Attacks for the Specific Layers	Counter Attacks for All Layers
Physical Layer	1) Secure Booting for all IoT devices a) Low power Cryptographic Hash Functions 2) Device Authentication using Low Power Techniques a) Data Integrity b) CRC – Cyclic Reduntancy Check c) Checsum d) Parity Bit e) WH Cryptographic Hash Function 3) Data Confidentiality a) Encryption Algorithms like Blowfish and RSA 4) Data Anonimity a) K- Anonimity	1) Risk Assessment b) Finding New Threats c) Applying Updates d) Applying Patches e) Providing Improvements f) Upgrading Systems 2) Intrusion Detection Mechanisms specific to IoT Systems 3) Securing the IoT Premises a) Physical Barriers b) Intrusion Detection Alarms c) Monitoring Devices d) Access Control Devices e) Security Personel 4) Trust Management a) Trust relation between layers b) Trust of Security and Privacy at each layer c) Trust betweeen IoT and User
Network Layer	1) Secure Communication between the devices a) Network Authentication – challenge-response mechanisms b) Point-to-Point Encryption for the confidentiality of the transmited Data c) Cryptographic Hash Functions for the Inegrity of the transmited Data 2) Implementation of Routing Security a) Use of Multiple Paths b) Encrypting Routing Tables c) Hashing Routing Tables 3) Secure User Data on the Devices a) Data Authentication b) Data Confidentiality; Encryption Schemes of encrypting the data c) Data Integrity; Cryptographic hash functions	
Application Layer	1) Data Security a) Authentication; biometrics, passwords, etc. b) Confidentiality; Strong Encryption Schemes (AES) c) Integrity; Cyrptographic Hash Functions 2) Access Control Lists (ACLs) 3) Firewalls 4) Protective Software a) Anti-virus b) Anti-adware	

Cybersecurity guidelines such as password policies, software updates, data transmission security, and network interfaces should minimise unauthenticated disclosures, protect device hardware against interfaces that threaten software integrity, make systems resilient to outages, and implement means of reporting vulnerabilities for consumer IoT as mentioned [105, 106, 107]. Most of these guidelines are for manufacturers of IoT devices before a consumer IoT device is sold. NIST further defines cybersecurity and privacy risks for IoT devices in terms of three high-level risk mitigation goals:

- Protect device security, which prevents a device from being conducting attacks or compromising other devices on the same network.
- Protect data security which protects the confidentiality, integrity, and/or availability of data stored on, collected by, processed by, or transmitted to and from the IoT device. This goal applies to each IoT device except the ones without any data that needs protection.

- Protect individuals' privacy which protects the privacy of a user. This goal applies to all IoT devices that impact users directly or indirectly [105].

Security has been and remains a key concern in IoT as IoT systems, as security breaches can risk not only the users' privacy but can also cause physical harm if connected devices are used maliciously. It is also a risk for manufacturers, since attackers could get access to sensitive information, and this could result in damage of the manufacturers reputation. The major objectives of IoT security are to ensure privacy, confidentiality, integrity, and availability of these services offered [34, 105, 123] tying back to what has been mentioned in NIST in the sections above. The following sections provide definitions in the context of IoT [123].

- Confidentiality: Confidential information must be protected against unauthorised exposure, either during transport or within storage.
- Privacy: Privacy and rights of individuals regarding the use of personal information are addressed.
- Integrity: Integrity in the IoT context is defined as ensuring data or message was not modified, or destroyed in transport, storage, or processing.
- Availability: Availability refers to systems and services being available when required.

Commercial trends for protecting against the attacks caused by compromising the above revolve mainly around detecting and preventive measures, such as encryption or two-factor authentication. However, these have not been validated as successful measures [92].

Karie *et al.* [110] comprehensively evaluated security standards and assessment frameworks that can be implemented in smart home frameworks which included several NIST special publications on security techniques, including the NIST SP 800–53 series, International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) ISO/IEC security standards, including the ISO/IEC 27000-series of standards, 32 ETSI standards and 37 different conventional security assessment frameworks. The evaluation included both security standards and assessment frameworks as well as those under development. The results showed that most of the conventional security standards and assessment frameworks did not address

the security needs of smart home environments. Bahizad [132] in his paper assessed security risk frameworks such as STRIDE, CVSS, Octave, NIST, ISO and FAIR and discussed that these security frameworks, due to the complexity of IoT systems, are unable to include all the different aspects of IoT and there are no frameworks specifically developed for IoT.

A study conducted in [9] found many risks associated with users in which smart cameras broadcast sensitive data, including geographical locations and even username and password combinations. In addition, for non-technical users, this is bothersome, especially as users do not know how to protect themselves from intruders. This lack of awareness demands a redesign of smart home configuration tools and interfaces and correlates to the generic threats caused by user unawareness [24]. An important design consideration is that not all users are not technologically inclined, and many would not be aware of the risks that smart home IoT devices bring forward. Given the increasing number of real-life incidents of smart homes device invasions, user awareness of threats to their smart home environments is crucial.

Several research has analysed how IoT sensors are added to smart home network and several research have investigated ways to make devices safe from a technical point of view. Overall, it was determined that security of these devices should be a priority. When customers purchase these smart home devices, they want to connect to other devices within the smart home network. Some authors have argued that users are responsible for their own devices and their protection. The user is, in essence, responsible for knowing what kind of information can be used when connecting devices and understanding potential intrusions so that they do not put their privacy at risk [111, 124]. To help address this, Hammi *et al.* [112] proposed a taxonomy of security requirements, challenges, and cyber-attacks on smart home environments as shown in Figure 2.10.

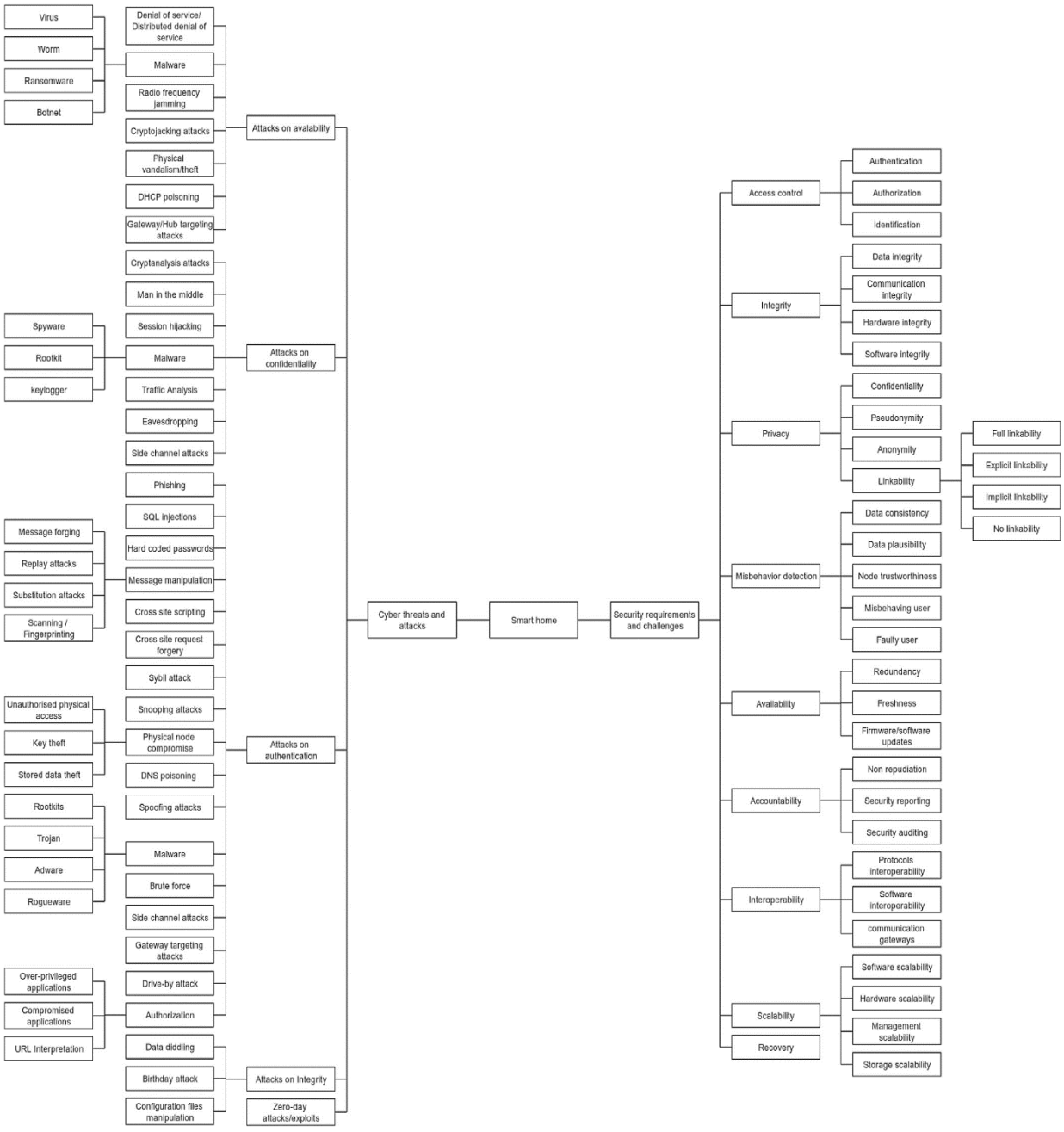


Figure 2.10: Smart home attacks, requirements and challenges

Systems that detect intrusions are known as intrusion detection systems (IDSs). These systems detect intrusions and alert users of an intrusion that is occurring. IDSs are defined as a software or hardware product that monitors and analyses the process of detecting intrusions in a system or on a network and alerts users of these intrusions [21, 36, 53] using specific methodologies. In the context of this research, IDSs are systems that uses the help of the users to detect intrusions in a smart home IoT environment and alerts them of the intrusion that is happening within their smart home internal network.

IDSs in IoT has been proposed and investigated, and many IDS frameworks have been adopted to detect intrusions [15, 17, 19, 20, 26, 100, 124, 125, 126]. Most IoT smart home devices have limited resources and adding in more capabilities introduces more challenges for security and privacy [124].

As the whole of smart home internal network is considered which may or may not consist of more than one device, a NIDS will be considered for this research. As all users may not be technical savvy and the intrusion that occurs within their smart home internal network will also be different, the scope of this research is detection and alerting the user of an intrusion and not intrusion prevention or mitigation.

Due to the development of threats, it is imperative to raise security awareness among users and specifically among smart home users [8].

2.4 Conclusion

This chapter provided a brief overview of IoT building blocks and led to the three-layered frameworks that are followed to build any IoT model or infrastructure. It then gave an overview of the attacks that could occur at each layer of IoT and the countermeasures that could be provided. The study in security leads to many issues mainly focusing on where users would be most vulnerable, which is the smart home environment, and the generic threats and user unawareness.

The possibilities of IoT are vast and so are the risks that come with it. Smart home appliances connected to IoT impose higher risks to privacy and personal data and information. Since making users aware of security and having them have control of IoT devices was crucial in bringing the best out of smart home devices, an acceptable approach to alert users if an intrusion has occurred in their smart home environment was IDSs. Due to the number of threats emerging, user awareness and security offered to the user is necessary. Bringing in user involvement and user awareness was considered a gap by many literatures. The main goal of this research is to develop a design involving users and making use of an IDS to alert them of security breaches. Hence, the next chapter focuses on exploring existing research that enables user configurations to protect smart home internal network.

3
IoT IDSs & Smart home security frameworks

This chapter explores the existing research done in the analysis of the security of the smart home environment and highlights the security solutions proposed in smart home environments and their limitations. The chapter further explores the IDSs used in the smart home environment and analyses the method with which intrusions are identified. The capabilities and limitations are proposed in this literature.

3.1 Existing research on IoT frameworks

Hammi *et al*. [112] provided a holistic view and comprehensive analysis of the security of the smart home environments. Different cyberattacks and threats, with security and safety requirements and challenges were discussed and a taxonomy provided for it. A survey of recently proposed security solutions was also provided with recommendations that can help smart homes. The findings from the survey indicated that many of the recent publications on the topic of smart home security are briefed, with many of them covering only a few security and threat aspects. As such, they cannot be considered extensive surveys. Furthermore, many surveys are not dedicated to smart homes but rather considered as IoT-use cases. They should be dealt with as such. Finally, it was discussed that many of the commercial products of the smart home market are the origin of most of the known security faults. Several academic papers, company white papers, case studies; and surveys were evaluated for this purpose. It was concluded that most of the smart home systems are vulnerable to a wide variety of cyberattacks and that none

of the formerly proposed smart security home architectures has considered the different security challenges and issues.

Many research papers included surveys that discussed privacy and security challenges in the IoT. Only limited research addressed access control, which is the authorised access of the systems. However, these surveys did not cover all aspects of access control and thus does not summarise the smart home requirements of access control [101].

This research also conducted a brief literature survey on the existing smart home security. Mohammed *et al.* presents an overview of the current access control solutions for smart homes in their survey. Their evaluation is based on specified requirements of which multiuser management and access control systems allow users to easily manage the policies that are relevant to this research. From their survey present in [101], it was noted that the research that took consideration of the management policies in ensuring security as well as multiuser management, were very few. The paper also discussed that multiuser management, and flexibility of users regarding access control by using smart home networks, was a great challenge even for future smart home networks.

Kuyucu *et al.* [127] and Williams *et al*. [128] discussed a survey on smart home security systems; privacy; and security issues in existing literature. The survey considered security based on communication technology, infrastructure and pre-determined user behaviour, and security mostly taking into consideration a single user. They suggested that these domains should include a user interface and that smart home designs should take into consideration more than one user living in the smart home.

Lourme *et al.* [129] discussed what an IDS in a smart home environment should consider in their research. The lack of technical skills of smart home users was mentioned as a major challenge for security and privacy. The IDS should be designed simple enough for the user and the user should be notified when an intrusion takes place.

Other related work on IDS use in smart home environments is presented in the table below. The contributions and limitations of the research is provided below.

Table 3.1: IDSs used in smart home environments

Ref.	Year	Scope	Contribution	Limitation
134	2020	Intrusion detection system in smart home network using artificial immune system and extreme learning machine hybrid approach	The paper presents early work of an IDS by detecting anomalies in the smart home network, using Extreme Learning Machine and Artificial Immune System (AIS-ELM). AIS uses an input parameter and based on the input parameter ELM detects intrusions.	Intrusion is detected based on a certain input parameter. What the parameter is, is not clearly defined. The AI system does not learn anything about users. Users are not involved, how the users are alerted, and a mitigation strategy is not proposed.
100	2019	Anomaly detection models for smart home security	Behavioural data and Network data is collected, and a hidden Markov model is trained to detect intrusions. This is discussed below in more detail in section 3.1.6	Only applicable for a single occupant in a smart home. Users are not involved in security but only a single user's behaviour is learned to detect intrusions. How the user is alerted, and a mitigation strategy is not proposed.
135	2021	Intrusion detection system in smart home network using bidirectional LSTM and convolutional neural networks hybrid model	The research presented an IDS that detects network anomalies using trained network characteristics that uses a bidirectional long short-term memory (BiLSTM) and convolutional neural network (CNN) hybrid model. Intrusion is detected based on device behaviour that is different to what has been learned.	Users are not involved, and a mitigation strategy has not been proposed.
136	2020	HID-SMART: hybrid intrusion detection model for smart home	The research proposes a Hybrid Intrusion Detection (HID) system using a random forest algorithm and misuse detection by using network and user behaviour.	Users are not involved, and user behaviour is based on a single user. How the users are alerted, and a mitigation strategy is not proposed.
137	2021	Behaviour-rule specification-based ids for safety-related embedded devices in smart home	The paper proposed a behaviour rule specification-based IDS to detect intrusions based on specified behaviour on the device activity.	Users are not involved. How the users are alerted, and a mitigation strategy is not proposed.

IDSs that has user involvement is discussed in the sections that follow.

3.1.1 Behavioural framework for Smart Home

Shams *et al.* introduced gaming as a method to create user awareness and encourage user configurations in a smart home environment through the application of behavioural and motivational models such as Technology Threat Avoidance Theory (TTAT) and Fogg's Behavioural Motivation Model (FBM). The elements of the framework were then incorporated as a board game design. This was used to educate users about smart home device capabilities and enhance the configuration behaviour to inform users of privacy. How exactly these configurations are made possible, the impact of using these where multiple users are involved, and extracting the exact device capabilities, are beyond the scope of this research, however it is noteworthy that authors mention that more research is required to evaluate the scenario of using gaming to enhance awareness among users.

3.1.2 Supervised IDS for smart home

Anthi *et al.* [96] proposed an IDS for smart home IoT devices, which uses a three-layer IDS to detect intrusions based on the type and profile of the normal behaviour of the device in their paper. The system used standard machine learning classifiers to classify IoT activity as normal or intrusive. The features used were limited to network traffic including destination IP, protocol, and packet size. The authors classified the intrusions that have occurred based on supervised learning. Although a certain number of known intrusions were detected, an extensive period of training is required, which may not be practical for a smart home network. Moreover, this system is unable to provide alerts of intrusions, and there is no involvement of the users.

3.1.3 IOT-IDM using Open-Flow

Nobakht *et al.* [97] discussed a host-based intrusion detection system (HIDS) based on software-defined networking technology Open-Flow that provided intrusion detection and mitigation technology in smart homes. The features used for the detection are from network traffic. The signatures being used, and the exact mitigation strategy are unclear. However, the technique itself was based on known intrusion signatures and was tested against a single bulb. The viability of the research in multiple devices connected to smart

home networks was not established. Additionally, the research did not provide information on how signatures are formed and how users were involved.

3.1.4 Real-time DDoS detection in smart home

Procopiou *et al.* [98] proposed a lightweight algorithm based on chaos theory and prediction to detect flooding and distributed denial of service (DDoS) intrusions. For every series behaviour collected at a specific time, a forecast is generated, and the error of the forecast against the actual value is assessed to determine if it is, in fact, an intrusion. The actual detection is complex, as it evaluates the network for packets and traffic. With heterogeneous networks and the exact smart home network being unknown, detection could result in false positives. The research has not been extended for any available threats and does not show any user interaction or involvement.

3.1.5 Anomaly detection in user daily patterns in smart home

Novák *et al.* [99] discussed anomaly detection in unusually short and long activities carried out by users, specifically the elderly in a smart home environment using neural network with self-organising maps. Behavioural activities were captured and any activity deviating from it caused an alert. Although research involves users and could potentially enable users to live alone, this could cause privacy issues if these activities leak. Especially when the behavioural activities of users are captured.

3.1.6 Anomaly detection model for the smart home using Markov model

Ramapatruni *et al.* [100] employed a hidden Markov model-based approach that learns what is normal activity based on sensor data such as closing and opening a door and switching on and off a light bulb. Sensor data featured ‘closed’, ‘open’, ‘on’, and ‘off’ for each sensor. If the user is recognised as outside of their home (based on the Wi-Fi connectivity of their mobile device), then any activity related to the doors will result in an abnormal state. To test these activities within a smart home network, data was collected for three weeks, and then anomalous activities were determined from normal activities. This work shows that traffic from multiple sensors can be collected. To be used in every smart home, there will be a training period. Only a single user within a

smart home is considered and the research does not cover the use case when there is more than one user in the smart home.

3.1.7 COLIDE

Arshad *et al.* [102] described a collaborative intrusion detection framework (COLIDE) in their research, that is, an IDS that can be placed at the router level as well at the host level to detect intrusions, where 6LoWPAN is used. IDSs placed at the router level are able to block malicious traffic, and they do not consider the behaviour of the devices themselves. Smart home networks are different; hence, it may not work in all smart home environments.

3.1.8 SLASH framework

Sultan *et al.* in their paper SLASH (self-learning and adaptive smart home framework by integrating IoT with big data analytics) propose a framework for enabling smart adaptive home systems and self-learning, based on the occupant's behaviour. The framework suggests IoT smart home devices on a large network connected to a large data analyser. As the name suggests, the framework proposes a self-learning and adaptive smart home system. The device, for example, a light that is switched on by the inhabitant, learns the routine of the occupant. After several recurrences, the lights will be turned on when the occupant enters. To cover several scenarios of behaviour, many sensor readings must be provided by different occupants in the house. This information is then stored, analysed in a centralised system, and actions are taken based on each scenario. The SLASH framework uses large data analytics for decision making. To apply the SLASH framework, a component is required in each layer of the framework for each routine to be stored, analysed, and processed [55].

Although it is proposed that the framework allows easier scalability, maintainability, user-friendliness, and a combination of services. Privacy and security are major challenges for this framework. Private information of the user is recorded for each scenario and stored in the cloud. This framework does not discuss security within for its users.

3.1.9 EPIC framework

Liu *et al.* [57] discusses smart homes also becoming a medium for health care innovations in their paper. Where corporates are using IDSs as remote health systems based on smart homes. These remote health systems based on smart homes can access patient's health systems, caregivers can access patient's health status promptly and provide them with defensive instructions, helping to avoid emergency care and hospital admissions. This reduces a large amount of societal costs. The elderly prefers this, thus, there is a huge market for remote health monitoring systems in smart homes. In smart home health systems, all devices send private information and communicate with health care service providers through the Internet via a home wireless router (i.e., home gateway). The paper addresses the traffic analysis using a smart community, which is a smart network of connected smart homes. The EPIC framework focused on a resource constrained IoT environment and took advantage of the wirelessly connected smart homes to perform local traffic confusion for each smart home. The paper discussed a utility-optimal differential privacy mechanism to confuse the source of traffic flow by also allowing a multi-hop routing scheme. Therefore, the actual source or destination is concealed.

This paper further discussed a framework that aids in securing the private information of the user in a smart home by using obfuscation. However, once a proxy gateway is figured out by the intruder, all the information that is passed through is leaked and users are unaware of what will happen to their information or systems within the smart home.

3.1.10 Anomaly detection for smart home users

Yamauchi *et al.* [82] describes an anomaly detection method to detect intrusions for smart homes based on user behaviour in their paper. User behaviour is presented as a sequence of events. The method learns sequences of events for each of a predefined set of conditions and detects intrusions by comparing the sequences of the events with the learned sequences. This is managed through the home gateway. When a user behaves differently to the sequence of events, an intrusion is triggered. The paper provides a way to detect intrusions. How users can be alerted is unknown, and the framework does discuss how users will be made aware if devices behave without the knowledge of the

user. This paper does not highlight or discuss cases where there are several users in a smart home network, and how intrusions will be alerted.

3.1.11 COSMOS

Nespoli *et al.* [130] did an extensive analysis on the current IDSs proposed in smart homes in their research and concluded that much research defined specific proposals for the smart home scenario. The IDSs presented focused on core techniques such as anomaly or misuse detection and many used machine learning and artificial intelligence techniques. A lot of the research focused on detecting network attacks and were based on static conditions and only a few could adjust their operation to other factors like: the type of attack, topology, mobility conditions, network traffic, or devices capabilities. Many of these devices do not use the end nodes or devices within smart homes as well. The paper addressed that the solution proposed was the only solution specialised in smart home scenarios, that has detection capabilities, which was named as Collaborative Seamless and Adaptive Sentinel for the Internet of Things (COSMOS). The design states that COSMOS monitors network traffic and identifies any threats. A COSMOS sentinel is deployed in every smart home appliance while a Security Information and Event Management (SIEM) collects and analyses security events to detect massive and distributed attacks. This analysis allows the development of cyber threat intelligence information to prevent new attacks and to design a countermeasure mechanism. Many tools such as Suricata as the network IDS, Kismet as the Wireless IDS, and many others, were incorporated. They had existing signature databases to detect these intrusions occurring in COSMOS.

The architecture proved to be viable in using existing signature databases to detect known intrusions. It was noted that constrained resources, the numerous protocol stacks in IoT, present different ranges, openness, modulations, topologies, various threats at each layer of protocol stacks, several communication technologies, cost driven market without the importance of security and non-technical users, are all challenges in ensuring smart home security. The research further added that an ideal smart home IDS would ensure that it does not require complex actions from the user [103,104]. It is important to note that this would be applicable for any IDS proposed.

3.2 Existing IDS security frameworks vs. Research proposed

Most of the security research involving IDS or smart home security frameworks focused on authentication and access control [92,101]. Lately, there has been an increase in research tackling the challenge of detection. They have been two-fold: knowledge-based (using signatures of known attacks) or behaviour-based (detecting deviation from normal behaviour). Much of the research discussed above fall into these categories. The following was also noted:

- Detected specific type of attack
- Direct user involvement was much less or none. Including users to identify and configuring parameters to detect security, was not considered in most of this research.
- The use case of more than one user especially for user behaviour-based detection models in a smart home environment were not of focus.
- Although multiple devices were considered in some research, many did not consider the fact and the differences between them could cause the solution to fail.
- The focus was on specific network elements or technologies; thus, they may not work for all smart home environments.
- Intrusion detection using signatures only focused on known signature attacks. The interpretation of which rules they use and how they would be used in a smart home environment is lacking.
- How users were alerted was missed.
- There was no mitigation strategy for when an intrusion is detected.
- Many of these solutions are very complex and solutions may fail with the existing challenges of smart devices.

Unlike human-controlled computers, an intruder can easily access a smart device because of its continuous connectivity to the Internet. All these devices cannot afford to have security algorithms in their structure because of their small size, low cost, and portability. Most of these devices are handled by people without technical training and not by skilled engineers. Hence, making users aware of security in smart homes is an important factor.

The goal of this research is to develop a design that involves users to identify their smart home devices and configure parameters to detect intrusions using an IDS and to create alerts for intrusions detected, thus making users aware of security breaches. The research needs to consider existing limitations within the literature mentioned above. The limitations that are considered to ensure that the goal of this research do not have the same limitations are the following:

- Proposed solution should be applicable to a smart home environment where only one or more than one user is living.
- Since some of the research limitations that was pointed out are in detecting specific attacks only, and because the viability of using existing signature attack database was successful [130], this research will also incorporate a dataset of existing attack signatures to detect the most common network attacks in IoT. However, this should not become a complex task for users to perform.

Hence the security attacks and challenges that the proposed design addresses through user configurations based on the security attack and challenges proposed in [112] are as follow:

- Access control Identification, Node trustworthiness: identifying the devices within the smart home environment. External attacks can be identified by verifying that any other device from an outside network is not meant to connect to a specific node within the network.
- Security Reporting and Security Auditing: reporting on incidents that take place within the smart home as well as creating a log of events that occur in the smart home environment. Although this may not be helpful for non-technical users, it can be used in the event that a major intrusion takes place.

3.3 Conclusion

Many research papers provided risk assessments, threat modelling, and IDS frameworks and described the vulnerabilities and mitigations to certain attacks. These papers also identified that users are at risk when using smart devices. Researchers are starting to

address these security flaws and vulnerabilities in IoT devices, however, most of them are complex.

The smart home environment is complex and diverse security solutions that address all the required security aspects such as privacy, confidentiality and the integrity of a smart home. This is also complex and at present, consist of multiple systems that need to co-operate, e.g., COSMOS - one important system that is always present is an IDS. The configuration of the IDS to fit the diverse smart home environments requires user behavioural information. Different ways to obtain this behavioural information has been proposed in literature, e.g., using machine intelligence. The use of machine intelligence is proposed as a proxy for user involvement since it does not require user expertise. In our research, a simplification of smart home network complexities is proposed, in such a manner that a user can provide direct input into how they would require the smart home interactions to take place. Furthermore, continued interaction with the IDS through user configuration and event alerts, raises the user awareness of potential security threats.

4

Smart Home User Security Model through User Configuration

The aim of this chapter is to develop a design that involves users in detecting intrusions adapting the methodology of IDSs, so that they are aware of what is happening within their smart home environments. The solution should cater for multiple users or a single user and should be easy enough to be applied by both technical and non-technical users.

4.1 Design Methodology-SSADM

In the next section, the chapter proposes how the design is developed using the IoT project methodology as well as the structured system analysis and design methodology (SSADM) [90] as mentioned in Chapter 1. This chapter describes the design as developed through the different phases of the IoT project methodology as well as that of SSADM. The phases of SSADM are as follows: Investigation of the current system, proposed system options, requirements for the proposed research to resolve the issue of user security, logical design of the proposed design as well as the physical design of the proposed design.

The next section investigates smart homes by developing a threat model for smart homes and a presentation of the participation of users to identify what kind of intrusions should

be detected. The threat model falls under the section of analysing and interpreting data in a SSADM to identify the exact problem and the various components within a smart home environment to identify vulnerabilities and threats.

4.1.1 Brief threat model for the smart home

Ensuring internal security for the smart home is crucial in ensuring the physical security of users and the devices themselves when considering the installation and deployment of such smart home devices. Therefore, developing a threat model for home users who are often unaware of the threats to privacy and security, is the preliminary step towards improving security [12].

Kavallieratos *et al.* in their paper introduced a threat model for the smart home [13]. An evaluation of trust methodologies is also available [at 118]. The design proposed in this thesis adopts the methodology mentioned by Kavallieratos *et al.* Figure 4.1 shows the steps identifying threats at the user level.

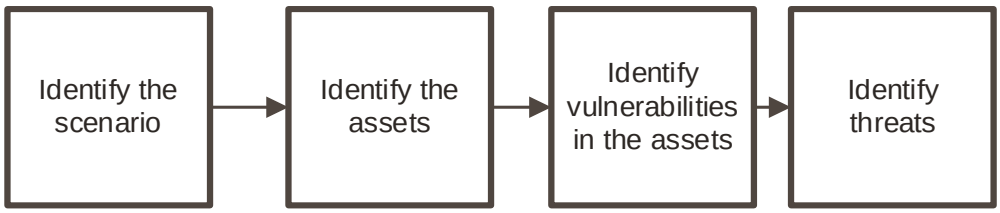


Figure 4.1: Threat Modelling

The steps used in the threat modelling are as follows: identify the scenario, the assets, vulnerabilities, and threats

Identify the scenario: A connection from an external network is made to a smart home device within the smart home environment which could result in an attack or compromise of the smart home device that the user inside the smart home is not aware of.

A connection from an internal smart home device that is compromised and connects to another device within the internal network that the user of the smart home is unaware of, is also a possibility.

Identify assets: All smart home physical devices are connected to a home network. This includes any smart home device connected inside the smart home internal network that is connected to a router, a hub, or a gateway to communicate to the outside network. Describing all available smart home devices available is out of the scope of this research. However, a list of the most common smart home devices per utility category based on market share and sales volume, can be found in the next table [19]. Any of these devices that may be present in a smart home environment can be identified as an asset. An asset might also be the privacy of the user, which can be compromised by the physical devices being attacked.

Table 4.1: Home devices [19]

Utility Categories	**Popular Devices**
Smart security Cameras	Amazon Cloud Cam, NetGear Arlo Q, Nest Cam
Cameras	IQ, Wyze Cam Pan, Google Nest Hello, Ring Video Doorbell, Arlo
Doorbell Cameras	Audio Doorbell
Smart Locks	Kwikset with Amazon Key, August Smart Lock Pro
Smart Speakers	Amazon Echo, Google Home Max, Apple's HomePod
Smart Hubs	Wink Hub 2, Samsung Smart Things Hub, Google Wi-Fi
Smart Light Bulbs	Philips Hue, GE C-Life Smart Bulbs
Smart Thermostats	Nest Thermostat E, Ecobee4 Smart thermostat
Smart switches	TP-Link HS200 smart Wi-Fi Light Switch
Smart Security Systems	Simple Safe, Ring
Smart Plugs	Belkin WeMo Insight Smart Plug, TP-link Kasa Smart Wi-Fi Plug, Amazon Smart Plug
Smart Smoke Detectors	Google Nest Protect, Ring Alarm
Smart Appliances	LG Signature Series Refrigerator, Samsung Electric Cooktop, LG Turbo Steam Washer and Dryer
Smart Vacuums	iRobot Roomba, Shark IQ Robot, ECOVACS DEEBOT

Identify vulnerabilities: Each of the identified assets has various security vulnerabilities, which have already been analysed and can be found in existing vulnerability databases [13]. The vulnerabilities of the prevailing smart home devices were classified into four categories, viz. physical, network, software, and encryption. [These can be found in [19]. The internal smart home network, if not protected circumspectly from the external network, could have vulnerabilities as well.

Identify threats: In this specific scenario, threats are those that occur by bypassing the router and accessing the smart home devices and taking control of them. The attacks

that could occur through the internal network are also threats. Many types of research, such as [3, 15, 16] described the attacks that could occur in the four categories, viz. physical, network, software, and encryption. A list of threats based on smart home architecture is provided in Chapter 2. While detecting all threats would be impossible, especially when more and more devices emerge, users can be alerted once a connection comes through to their devices in the smart home without their knowledge that compromises their privacy.

The risk of a connection taking place without the users' knowledge that compromises the devices and users' privacy is the threat on which this research focuses. The risk can be mitigated by involving the user to capture user configurations so that users are alerted when an unwanted connection takes place to the devices. The next section investigates a common smart home architecture and proposes system options and requirements.

4.1.2 System options and Logical design for the proposed research

The section below discusses the proposed system options, the requirements for the proposed research to resolve the issue of involving users in smart home security, and logical design of the proposed design in the SSADM. This section starts by presenting the system options.

For a smart home network, the architecture can be divided into three parts as per architectural design explained in Chapter 2: the internal network, the residential gateway or hub, and the external network [28]. When adapting the IDSs, it is important to notice where the IDS can be placed. Since the research does not focus on a specific device, the smart home environment, irrespective of devices, has to be monitored by the user. It is apt to place the IDS in the smart home internal network where smart home devices connect to a smart hub or router to connect to the Internet. Hence this IDS is a network IDS (NIDS). An IDS on the network is an IDS placed at the network layer of the TCP/IP stack, to monitor intrusions. A NIDS monitors the network traffic occurring within the smart home internal network and uses user configurations to determine whether a network connection is a risk or not, based on the configurations the user has captured.

Figure 4.2 shows the internal IDS framework for the smart home internal network. The smart hub controls the connections between the smart home devices internally to the

network and routes any traffic from the external network through to them, as shown with grey arrows in Figure 4.2. The NIDS component is placed within the smart hub, and communication between the hub, NIDS and its databases is represented with green arrows. The blue arrows between the devices represent actions that one device can take upon another. The hub itself could be protected using authentication mechanisms such as username, password, and two-factor authentication. The smart hub itself, the security of communication to the external network, the communication technology used within various smart home environments, is not in the scope of this research. This research focuses on the participation of users to configure parameters for their devices in a smart home environment using a hub/router. Rules are generated using this configuration together with a IoT dataset of existing attack signatures for the NIDS to detect intrusions and unwanted behaviour of nodes. The next section describes how intrusions can be detected.

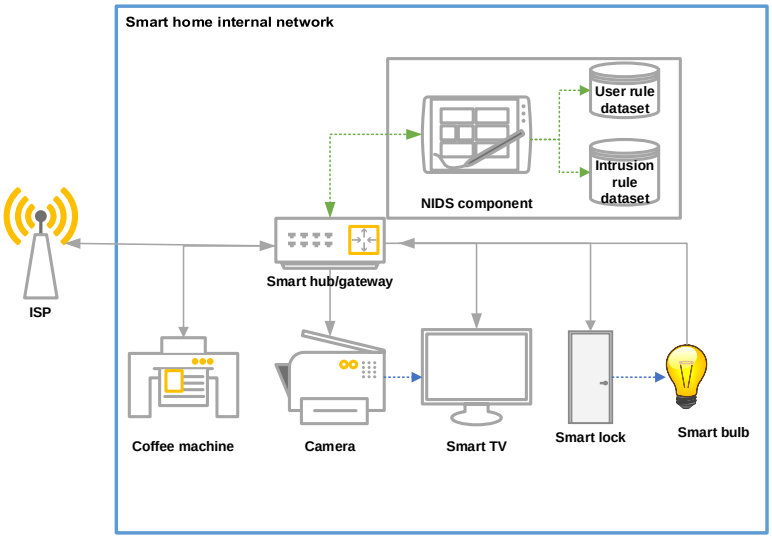


Figure 4.2: NIDS framework for the internal network of the smart home

4.1.2.1 Definition of user configurations for smart home devices

This section discusses the system requirements and requirements analysis for the system options in the SSADM and IoT project management, respectively. These configurations

must be presented in a user-friendly non-technical way since such users cannot be expected to know network parameters. The following process is proposed:

1) The user first identifies each device within the smart home by providing it with a unique name. This also helps in reporting back to the user in the event of an intrusion. The device names set up by the user can be in any form, for example, a smart home device clock can be represented as IoT1, coffee machine as IoT2, and so on.

2) The next task of the user is to establish whether that specific device can be triggered by another device. A trigger in the context of this paper is a device that releases a function to connect or activate another device. For example, a smart clock can trigger or initiate the coffee machine to start making coffee at a specific time. Therefore, the smart clock is allowed to make a connection with the coffee machine. Some devices, such as smart cameras are devices that should not be triggered by another device. Therefore, if the user has a smart camera, then the trigger device would be represented as of null value.

3) The next and most important parameter is the trigger method. The trigger method is stored as a number. The triggering method is captured so that the user knows that no other device or connection should happen to a specific device apart from what has been set up by the user. The triggering method can be of three types, and they are defined as follows.

- Manually triggered; represented as 0.
- Automatically triggered (auto triggered) at a certain time or due to an action; represented as 1.
- One device triggering another device; represented as 2.

The trigger method assesses each connection made to that specific device and evaluates if it is allowed, based on the trigger method. Thus, devices such as a camera will have a triggering method of zero. If a device ‘Clock’ is triggered automatically; this will be represented with an initiation method 1. If device ‘Clock’ is the trigger device for device ‘Coffee’, then the triggering method will be 2. The afore-mentioned configurations are the mandatory and basic configurations required to identify an intrusion.

In addition to these, other configurations that are not mandatory, even though the user may use them, are listed below. These configurations have not been used to build the prototype and are purely a suggestion and this is after receiving the test results of the prototype using the mandatory configurations.

1) The user may specify the time for a device when such a device can be active. An example here: if a smart door should only be active at a specific time and not at other times, then the time intervals at which it can be active should be specified, such as 07:00 am to 10:00 am. There may be more than one interval for a device. However, this may also depend on the users within the smart home and the usage of the device. Hence, a null value can be specified if the user wishes not to specify any time.

2) The next configuration that the user can specify is a remote media access control (MAC) address known to the user that can be entered to allow connections to a specific device. The hub must permit the incoming connection, and NIDS should not alert an intrusion in such cases that the incoming connection is the same as the one which the user specified.

The user should be able to define user configurations through a user interface of the smart hub. Configurations must be applicable to any device within an internal network, irrespective of the number of users.

As an example, consider the user configurations below.

Table 4.2: Rule sets of user rules

The device clock is auto triggered and not by any device. Therefore, the trigger method is 1. There is no specific time that the user has set up for the device and no remote connections or password set up for the device; hence there are no other rules for the specific device.	0/clock/1
The device switch is manually triggered and not by another device. Hence, the triggering method is 0. The device time specified is between 7:00 am and 10:00 pm. Hence, any connections made	0/switch/0/

outside of this time should be triggered as an intrusion. There is no remote connection specified.	
The device door is manually triggered and not by any other device. There is no specified time for the device. There is a remote MAC address that is specified; hence all connections taking place from that remote MAC address should be allowed.	0/door/0

However, these user configurations defined above are not yet in a format that can be used by the IDS. User configurations must be translated into a format that allows IDS to detect intrusions. The translation of user configurations into rules is described in the next section.

4.1.2.2 Generating rules from user configuration

Rules are generated from configurations that are mandatory because non-mandatory configurations may not have a value. These rules are generated so that the NIDS can use them. The smart hub allows or disallows connections using configurations that are not mandatory.

To generate rules from user configurations, this proposed design evaluated the rules of the IoT network dataset as well as the SNORT intrusion detection system, so that an IDS or IoT based-rule syntax is followed. The IoT network dataset rules do not have a defined syntax, while snort rules do. The proposed design adapts some of the syntaxes of the snort rule IDS as snort rules have a defined syntax on how the rules are formulated. More information on snort rules can be found in [62].

Snort rules have three parts: a rule header which defines the IP address, port, and protocol details using actions such as *alert, log,* and *pass where the* action words are: in *alert*: *alerts* and *logs* the packet, *log*: *logs* the packet, and *pass*: *drops* or *ignores* the packet. The rule action follows the rule header, which is the attack signatures, and the 'msg'- part, which is the response mechanism. The rule header syntax and specifically that of the actions, is what is adapted in this study to generate rules out-of-user configurations. The syntax part of attack signatures and response is not needed to

generate rules out-of-user configuration. For example, consider the snort rules below: the contents up to the first parentheses, form the rule header. The rest of the rule after the first parentheses, forms the rule option.

- alert tcp 193.35.64.2/30 80 -> 130.165.13.8/25 121 (content:‘‘| 00 01 86 a5|‖; msg:‖mountd access‖;)
- alert tcp any any -> 130.160.13.2/24 any (flags: A; ack: 0: msg: NMAP TCP PING‖;)

The action part of the rules starts with the protocol. In Figure 4.3, in the first rule, the protocol is ‘tcp’. The protocol is followed by the IP address and port number. The first IP address followed by the protocol is the source IP address, and the IP address and port number specified after the arrow is the destination IP address and port number. In Figure 4.3, the source IP address is 192.34.64.2/30, which specifies any IP address in the range of 192.34.64.1 to 192.34.64.30 using a port number 80. In the second rule, the source IP address and port number are specified as ‘any’, which means any source IP address and any port number. The IP address after the source IP address is the destination IP address, which is specified as 130.165.13.2/24.

The same method for specifying a range of IP addresses can also be used if the dynamic host configuration protocol (DHCP), which, in a smart home internal network, is DHCP. In this study, the known IP address is that of the smart home devices within the internal smart home internal network. However, the IP address alone is not sufficient enough to identify a device, and hence the smart hub and IDS should also know the MAC address and ports of the devices. The triggering method, which is in the user configuration, is also used as per user configuration. If one device connects to another device within a smart home internal network, there could be a possibility that it could be an external device connecting to the smart home internal network, and the MAC address of that external device may not be known. Therefore, the MAC address identified the source devices, which are devices within the smart home, which is also used as a rule. The known port numbers are used as a rule or can be specified using any. Protocols are not used, as many devices could use different protocols.

These devices within the internal network of the smart home are the destination devices which intrusions can trigger. From a source device which connects to the destination

devices, the same information, such as all network details, may or may not be known. Hence, some information may be optional when rules are generated. Rules can also be generated for remote IP addresses that the user is aware of and that are allowed to connect to a specific device within the smart home.

The user configurations define connections that can be permitted to connect to a device. Similarly, remote connections that are permitted, are also not intrusions. These rules are generated using the keyword 'pass' and called **direct** rules. Any other connections that take place, which would be considered unauthorised access, should be flagged as an intrusion. These rules are created using the keyword "alert" and are called **indirect** rules. These rules are kept in the user – rule data set. The rule syntax of the rules created, based on the user configurations, has the following format.

Pass or alert <any/ source IP address> /<any port number> <destination IP address\range>/<MAC address>/<port number>/<triggering method>

If any parameter is unknown, it is represented using 'any' as in the SNORT rule. Imagine then that the device has a time specified and a remote IP address specified, as well as a password. Then direct rules are created with triggering method 2 as below.

Pass192.168.0.3/1025/192.168.0.4/00-F0-56-F2-B5- 12/1026/2

The above rule states that a connection from the source IP address 192.168.0.3 using port 1025 may be connected to device 192.168.0.4 with MAC address 00-F0-56-F2-B5-12 – then using port 1026, trigger method 2 should be passed or allowed. This means that only a specific source device can trigger a connection to the destination device using triggering method 2. Since this connection is allowed, it is a **direct** rule.

The remote IP address specified 132.178.0.1 will also result in a rule as below, as this connection should be allowed.

Pass132.178.0.1/any/192.168.0.4/00-F0-56-F2-B5- 12/1026/any

The indirect rules created for the same destination node are shown below.

Alert any/192.168.0.4/00-F0-56-F2-B5-12/1026/2

Alert any/192.168.0.4/00-F0-56-F2-B5-12/1026/1

Alert any/192.168.0.4/00-F0-56-F2-B5-12/1026/0

The rules state that any connection occurring to the destination device with IP address 192.168.0.4 with MAC address 00-F0-56-F2-B5-12 with port number 1026 and triggering method 1(auto-triggered) or 0(manually triggered) should not be allowed and thus alerted as an intrusion. If a device should be manually triggered, then the user can create a rule for that device with a manual triggering method, which then will not create an indirect rule for manual triggering. In the above indirect rule, the device has a rule that no manual triggering is allowed.

If a DHCP server is used in the smart home internal network, then the IP address range within the internal network should be known and can be specified in the rule. The MAC address will also ensure the identification of the specific device. The triggering method plays a vital role in the rules to determine the way connections should take place on a device and should detect intrusions this way.

The hub will allow or disallow connections using any time specified for the specific device and any remote MAC address that is specified for the particular device.

Two-factor authentication should be applied on the smart hub, where every connection that takes place between devices should provide the password set by the user on the hub for a connection to be allowed. However, as mentioned before, security of the individual components of the smart home infrastructure, is outside the scope of this study. IDS alerts the user once an intrusion is detected. When a new device is added, the user can add the configuration for that specific device. New configurations will not affect existing configurations of any other device or the rules of any other device.

Below are examples of some of the direct and indirect rules created, based on the basic and mandatory user configurations.

Table 4.3: Rule sets of user rules

User configuration.	**Direct rule**	**Possible rules**
0/clock/1	Pass 192.168.0.1/1024/192.168.0.1/00-D0-56-F2-B5-12/1024/1	Alert any 192.168.0.1/00-D0-56-F2-B5-12/1024/0 Alert any 192.168.0.1/00-D0-56-F2-B5-12/1024/2
0/switch/0	Pass 192.168.0.2/80/192.168.0.2/00-E0-56-F2-B5-12/80/0	Alert any 192.168.0.2/00-E0-56-F2-B5-12/80/0 Alert any 192.168.0./00-E0-56-F2-B5-12/80/2
Fridge/coffee/2	Pass 192.168.0.3/1025/192.168.0.4/00-F0-56-F2-B5-12/1026/2	Alert any 192.168.0.4/00-F0-56-F2-B5-12/1026/1 Alert any 192.168.0.4/00-F0-56-F2-B5-12/1026/0
Camera/fridge/2	Pass 192.168.0.5/1027/192.168.0.3/00-G0-56-F2-B5-12/1026/2	Alert any 192.168.0.3/00-G0-56-F2-B5-12/1026/1 Alert any 192.168.0.3/00-G0-56-F2-B5-12/1026/0
Door/camera/2	Pass 192.168.0.6/1028/192.168.0.5/00-H0-56-F2-B5-12/1027/2	Alert any 192.168.0.5/00-H0-56-F2-B5-12/1027/1 Alert any 192.168.0.5/00-H0-56-F2-B5-12/1027/0
0/door/0	Pass 192.168.0.6/1028 192.168.0.6/00-I0-56-F2-B5-12/1028/0	Alert any 192.168.0.6/00-I0-56-F2-B5-12/102/1

		Alert any 192.168.0.6/00-I0-56-F2-B5-12/1028/0

These rules are kept in the user rule data set. If the user changes any of the configurations, then the rules created previously for the device, should be auto- deleted, and new rules created based on the user configurations.

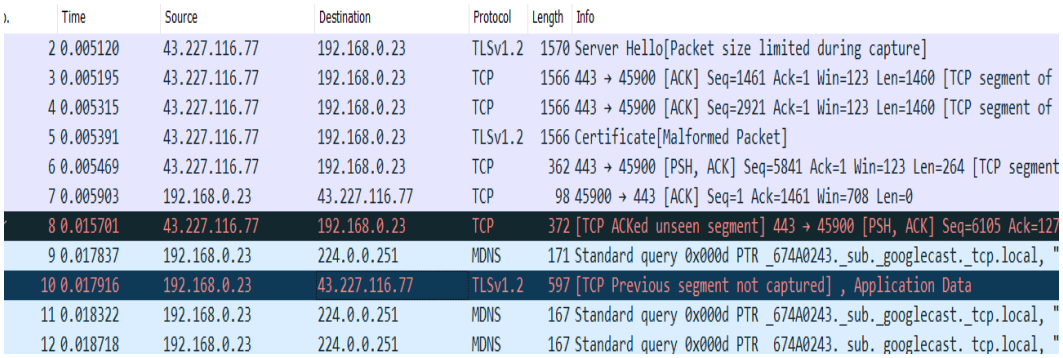
The IDSs have a separate mechanism to capture the log of all transactions taking place. Therefore, the log-action word is not used. The IDS also alerts users once an intrusion is detected. However, these rules are not enough to identify threats, as discussed in the threat model. Hence, attack signature rules are also required to identify attacks, which is explained in the next section.

4.1.2.3 Intrusion data set

In addition to these user configurations, known attack signatures are used as an additional security mechanism to detect known intrusions such as DoS, malicious code injection, Mirai botnet, and scanning. The standard IoT network dataset [88] released by the IoT security community in conjunction with IEEE, is used unchanged in our work to detect security attacks. The IoT network dataset consists of 137,986 packets of various attack signatures. These rules are kept in the intrusion dataset to detect known attacks. These rules are kept in the intrusion dataset to detect specific attacks. A sample rule from the IoT network dataset [88] is represented below. The full IoT network dataset with the attacks labelled can be found at [88].

ip.src == 192.168.0.15 and ip.dst == 192.168.0.13 and ((tcp.flags.syn == 1 and tcp.window_size == 1024) or tcp.flags.reset == 1)

The IoT network connections in the IoT network dataset was interpreted through a network sniffer tool as shown in Figure 4.3.



No.	Time	Source	Destination	Protocol	Length	Info
2	0.005120	43.227.116.77	192.168.0.23	TLSv1.2	1570	Server Hello[Packet size limited during capture]
3	0.005195	43.227.116.77	192.168.0.23	TCP	1566	443 → 45900 [ACK] Seq=1461 Ack=1 Win=123 Len=1460 [TCP segment of
4	0.005315	43.227.116.77	192.168.0.23	TCP	1566	443 → 45900 [ACK] Seq=2921 Ack=1 Win=123 Len=1460 [TCP segment of
5	0.005391	43.227.116.77	192.168.0.23	TLSv1.2	1566	Certificate[Malformed Packet]
6	0.005469	43.227.116.77	192.168.0.23	TCP	362	443 → 45900 [PSH, ACK] Seq=5841 Ack=1 Win=123 Len=264 [TCP segment
7	0.005903	192.168.0.23	43.227.116.77	TCP	98	45900 → 443 [ACK] Seq=1 Ack=1461 Win=708 Len=0
8	0.015701	43.227.116.77	192.168.0.23	TCP	372	[TCP ACKed unseen segment] 443 → 45900 [PSH, ACK] Seq=6105 Ack=127
9	0.017837	192.168.0.23	224.0.0.251	MDNS	171	Standard query 0x000d PTR _674A0243._sub._googlecast._tcp.local, "
10	0.017916	192.168.0.23	43.227.116.77	TLSv1.2	597	[TCP Previous segment not captured] , Application Data
11	0.018322	192.168.0.23	224.0.0.251	MDNS	167	Standard query 0x000d PTR _674A0243._sub._googlecast._tcp.local, "
12	0.018718	192.168.0.23	224.0.0.251	MDNS	167	Standard query 0x000d PTR _674A0243._sub._googlecast._tcp.local, "

Figure 4.3: IoT network dataset connections

The user rule dataset and the intrusion dataset are used by the IDS to detect intrusions and to alert the user on the smart hub user interface.

Figure 4.4 shows the data flow within the proposed internal smart home internal network. In the data flow, the user enters configurations that create rules in the user rule dataset. The IoT intrusion dataset is also available in the NIDS on the smart hub. When an external connection attempt occurs to connect to any of the devices, the smart hub verifies whether that specific device can be connected to that specific device. If it cannot, then it should not allow the connection. If it can, then the smart hub verifies if it is from a MAC address that is specified. If it is, then it should allow the connection. If it is not, then the NIDS verifies the connection against the datasets to validate whether it is an intrusion based on rules created with the mandatory configurations. The direct rules are checked, followed by the indirect rules. If it is an intrusion, then it is alerted. If it is a normal connection, then the connection is allowed.

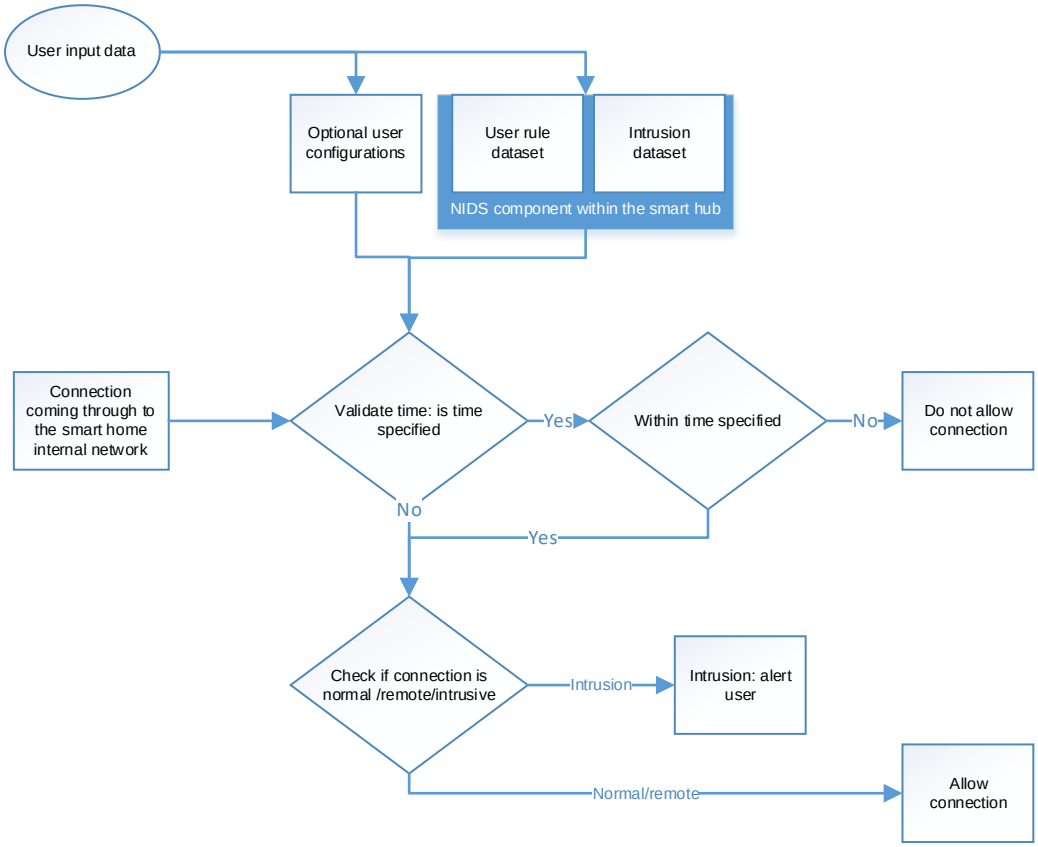


Figure 4.4: Intrusion detection data flow

4.1.3 Design achievement

The proposed design uses both the rules configured by the smart home user and the parameters from the network connection. The design was evaluated based on gaps after analysing the existing research mentioned in Chapter 3. The achievements mentioned below represent the achievements of the logical design in the SSADM methodology and tie into the threat analysis by mitigating the threats identified in the threat analysis.

Table 4.4: Achievements of logical design

Develop a design that involves the user to identify the devices within their smart home and which can configure for their smart home environment.	The user configuration was introduced in the design of the smart home internal network. Configurations are based on devices and a user can set up configurations for the smart home.

Create a seamless user configuration that any user can use with their smart home devices to detect intrusions happening.	The user configurations are simple and not complex and can be managed by even non-technical users. The back end creates the rules to detect intrusions from these configurations.
Alert users of intrusions within their smart home environment using their configurations irrespective of device, number of users, or smart home network.	The rules do not consider device profiles or the number of users. It uses features that are common to all devices to detect intrusions. Configuration features are also irrelevant to the number of users, and features such as time were purposely left out to accommodate the number of users.
In addition, one should use existing attack signatures to target the most common attacks.	The IoT network dataset that has known attack signatures was also introduced in addition to the configuration rules to detect known intrusions.

The proposed system makes the user aware by alerting users if any external connection is made to their smart home. Users are asked to identify and name their devices. The IP addresses used by the devices inside the smart home system are known to the smart hub and the IDS. Users can define a known or remote MAC address that needs to connect to the internal smart home network through the user configurations; hence only systems that are not known to the user connecting to the smart home devices will be identified as an intrusion.

Once the logic design was achieved, the research evaluated building a physical design. The conversion of the logical design into a working product is achieved through the physical design. In this research, the physical design is achieved through a prototype as discussed in Chapter 5. SSADM does not stipulate specific security rules as the approach could be used for any project. However, since this research involves security, a secure design was considered for the prototype in the next section by following the NIST standards for IoT.

4.2 Security considerations for the physical design

There are many secure design methodologies with a wide range of applications. Secure system design methods have evolved from checklists and standards to secure design methodologies. The idea of checklists is to identify possible countermeasures and to pick out security solutions. Checklists were followed by security standards such as ISO/IEC 17799, ISO/IEC 27002, and GAISP (Generally Accepted Information Security Principles). The distinction between checklists and standards is that the standards try to establish international, authoritative, and generic security standards. Because of the limitations of checklists and standards, security methods were developed. These methodologies can be classified into five categories: stepwise; object-oriented; viable; information modelling; and responsibility modelling. These methods are influenced by previous information systems (IS) and software development methods [139, 140].

The security methods take the previous methods such as checklists and standards, and adapt them in logical ways, using a repeatable process. Siponen [139] indicated that user participation and other user-centred design methods should be part of future secure information system design methods, which are pursued in the research presented in this thesis. This method confirms that the design meets the user's expectations.

A structural design process methodology was proposed by [140]. The basic idea of the methodology to secure a system is to protect its system assets on defined policies. An asset is a resource within the designed system. Security is only considered for resources that are required within the design. Resources which do not require security considerations are not the main concern of a secure design, but they need to be identified and documented. The methodology defined three phases as follows [140].

- Identifying assets
- Defining policies for securing each asset
- Enforcing the policies on the assets

Further secure design methods tried to incorporate security in the design flow diagrams (DFD) to improve the security of systems. A formal secure DFD (FSDFD) was proposed in [141]. FSDFD also secure each asset in a design such that the security of each asset will lead to a secured system.

Hence it was identified that the first step to designing a secure system is to specify the security requirements of the system [139,140,141], and then determine the security requirements of the identified assets of which the system is composed.

IoT security quality was also comprehensively described by [138] by defining a transparency model. The model provides a framework for the IoT security-quality metrics. The model was developed by mapping the security development lifecycle, followed by many organizations such as NIST, Microsoft, Synopsys, and PwC, onto the V-shaped product development process that many IoT vendors follow [138].

The model consists of the following:

- The "security by design" area consists of two parts: the process quality and the respective product quality. Those in charge of product planning and determining basic specifications are mainly responsible for this area. The goal is to provide a basic policy for providing a secure product that would earn the trust of users and define a basic process for implementing the policy. This is to allow users to trust in management's commitment to developing secure products.
- The "security assurance assessment" area involves the evaluation results. Those in charge of product development and quality assurance are responsible for this area.
- The "security production" phase details the items of security management during production. This is the responsibility of those that manufacture the product.
- The "security operation" phase includes the aftersales security monitoring and response to incidents. Those in charge of customer support, maintenance, and product security incident response team are responsible for this area.
- The "compliance with law, regulation, international standard" section implies that the public or industry requirements have been fulfilled. Compliance with industry standards and regulations is relevant to all areas.

In this study, a DFD was developed for the logical design. The design was then evaluated against the recommended security standards determined by NIST, for devices

and non-technical support for IoT following the secure design explained. NIST [133] defines an IoT product to refer to three specific components as follows:

- the networking/gateway hardware (e.g., a hub).
- Companion application software (e.g., the application to interact with the IoT device/devices).
- Backends (e.g., a cloud service, or multiple services, that may store and/or process data from the IoT device).

The transparency model and NIST IoT security controls were then adapted to develop a secure design for the physical design which aligns with the structural design methodology. This is explained in the next section.

4.2.1 Implementing a secure design.

The logical design was evaluated against the transparency model and structural design methodology to plan for a physical design, the prototype. Since the physical design will be a prototype, security by design and security assurance assessment are the main factors that need to be considered for the physical design. The rest of the components in the transparency model do not apply to the prototype and apply to a commercial product hence will not be considered as part of the research. Defining policies of the assets and enforcing policies from the structural design methodology is also applied in the sections that follow.

Security by design: Security by design is to provide basic security in product planning. This research adapted the NIST security requirements to evaluate the basic security of the prototype as the first step as well as defining and enforcing secure policies of the assets as explained in the sections that follow.

In this research, the backends are not within the scope of the research, so it is assumed that security standards are met for the external network as per general security measures and the evaluation of these standards in Chapter 2. The gateway or the hub is where the user interface application resides, and the smart home devices are part of the internal network; hence, security standards must be met for both. Security standards to be met for IoT products include the following: hubs and smart home devices such as device identification, device configuration, device protection, logical access to interfaces, and

the cyber-security state awareness that can make information available and accessible to authorised entities only; these have been explained in NIST and lie with the manufacturers of the devices. The non-technical measures in terms of documentation, queries and information broadcasting, can be found in the NIST publications that the manufacturers of these devices need to adhere to.

The IDS has not been changed and adapted, and the security standards of IDS as mentioned by NIST [135], must be taken into consideration. These were the security requirements that needed to be documented but were not necessarily required for the security of the prototype.

The application proposed by the research that resides in the hub is protected by the security standards of the hub. The IoT devices, if in real-time, would have to follow the security controls proposed by NIST; however, in this research, the devices are simulated as part of the application.

The basic security controls of NIST were also followed for the physical design to implement a secure design of the prototype and to enforce security policies for the assets that require security. The following controls described by NIST [133, 134] were adapted.

1. Access control and authentication

- Authorised entities to have access to the application.
- Authorised entities to configure authentication mechanisms (e.g., minimum password length or complexity, force change of passwords on first use)
- Authorised entities to only configure rules.
- Authorised entities to enable or disable notification when an update is available and specify who or what is to be notified.

The above controls will be validated as the application will reside on a local PC that can only be accessed by authorized users. Moreover, the application itself has authentication where users need to log in to access the application.

2. Data storage

- Ability to cryptographically store passwords at rest, as well as device identity and other authentication data.
- Ability to support data encryption and signing to prevent data from being altered in storage.
- Ability to secure data in the device storage.
- Ability to use separate storage partitions for system and user data.

The password storage will be securely protected by existing secure rules of the device in which the application resides. The application will not be made available or accessible to any other users apart from the PC it is using.

3. Transmission of data

- External applications cannot discover or connect to the application.
- The application only communicates to the IDS and hub.
- Cryptographic algorithms should be used to protect data in transit.
- Ability to use one or more capabilities to protect the data it transmits from unauthorised access and modification.

The device will act as a both client and server, hence there will be a minimal transmission of data outside of the PC in which the application resides.

4. Auditing and monitoring

- Ability to generate an audit log for transactions happening.
- Ability to alert users of any password changes.

An audit log will be created and presented in the coming chapters for transactions that could occur. All password changes abided by the existing security rules of the PC in which the application resided and allowed for notifications.

4.3 Conclusion

The chapter proposed a design where users can identify their devices and incorporate user configuration to alert them of intrusions, thus making them aware of security

breaches within their smart home devices. The chapter explained in detail the smart home network environment, the research proposed and user configurations that users can use to detect intrusions occurring at the device level and within the network. The design was then evaluated compared to the gaps found in existing research and it then explained how the design tried to alleviate these gaps. Security concepts were considered for the design. The next chapter evaluates the design through a feasibility study and a prototype.

5
Design using User Involvement–A prototype

This chapter discusses the prototype that simulates how users can control their smart home devices and get notified, as and when required, when their smart home devices are working whilst providing security controls per the design mentioned in the previous chapter.

5.1 Prototype installation requirements and functions

Table 5.1 below captures the development preparation and hardware and software requirements in the IoT project methodology. The software environment, platform, and configurations in which the prototype was developed are explained. The first column corresponds to the software artefact, and the second column showcases the specific platform, version, and configurations on which the prototype was conceived.

Table 5.1: Software environment, platform, and configurations

Operating systems	Windows 10, 64-bit
Programming language	Python 3.7
Python tools/packages used	PIP, Pandas, Matplotlib, Numpy, Scipy

Integrated Development Environment (IDE)	PyCharm Community Edition
Graphical User Interface (GUI) development	Python Tkinter GUI Development Kit

The system requirements for the prototype or a system that requires PyCharm are mentioned in the table below.

Table 5.2: System Requirements [83]

Requirement	**Minimum**	**Recommended**
RAM	4GB of free RAM	8 GB of total system RAM.
Disk space	2.5GB and another 1GB for caches	SSD (solid-state drive) with at least 5 GB of free space.
Monitor resolution	1024x768	1920×1080
Operating system	Microsoft Windows 8 or and advanced version MacOS 10.13 or an advanced version. Linux distribution that supports Gnome, KDE or Unity DE. Pre-release versions are not supported.	The latest 64-bit version of Windows, macOS, or Linux (for example, Debian, Ubuntu, or RHEL).

PyCharm is a IDE that functions on multiple platforms such as Windows, macOS, and Linux operating systems. PyCharm is obtainable in three editions: Professional,

Community, and Edu. The Community and Edu editions are open-source projects, although they have fewer features than the Professional edition [83].

Python has several GUI frameworks, but Tkinter is the only framework built into the Python standard library. Tkinter works on multiple platforms, so the same code works on Windows, macOS, and Linux. Visual elements of Tkinter are rendered using native operating system elements, so applications built with Tkinter does not look different to the platform where they are run [84].

As mentioned in the research, the prototype showcases user involvement in identifying the devices, enabling users to configure parameters that are then converted to rules. The rules subsequently detect intrusions and alert the users. An additional IoT intrusion dataset is also incorporated to detect attacks. When an intrusion occurs, the user is alerted. The intrusion detection functionality is adapted through settings managed by the users ensuring they are alerted. The differences in the heterogeneous environment, such as different communication protocols and differences in devices, are not in the scope of this study. The prototype requires network connectivity and uses the TCP/IP communication protocol. The prototype functions and modules are explained in detail in the following sections.

- **Smart home IoT devices**

As alluded to in previous chapters, IoT devices highlight two or more devices that connect and communicate with each other and a smart hub, such as a router or gateway. It is this hub that monitors the connection between these devices. For the prototype simulation, six IoT devices are modelled using a client-server architecture, where the client acts as the smart home device and the server as the smart hub.

- **Smart hub**

The smart hub is an advanced gateway or router that is either software or hardware that can connect to various devices and control them. It can also be a hosted service in the cloud and connects to the IoT application and devices. In essence, the smart hub correlates and manages the IoT devices and applies various security controls, including identity, authentication, and authorisation. For this prototype, the smart hub is a software

simulation module which was developed and runs behind an IoT application and acts as the server that facilitates the connection of the smart home devices.

The focus of this research is not to develop or deploy a smart home environment but rather a feasibility study and a prototype; hence the standards and frameworks mentioned in Chapter 2 have not been comprehensively applied. Chapter 2 gave an overview of the security standards mentioned for the hub, consumer IoT devices and IDSs; however, the prototype developed in this study illustrates a feasible solution. However, it has not yet been subjected to the rigour required for commercial deployment.

The software development of the prototype happened in a secure environment as per existing security standards and was developed on a local device. The application developed to test the user rules did not connect externally to the network apart from the local device being able to connect to the external network.

5.2 The prototype

The prototype intends to let the users decide how their devices should behave and alert them if the devices communicate in a manner that is different from what the user has set up. In the SSADM, the prototype serves as the physical design of the logical design mentioned in Chapter 4.

The prototype is developed to satisfy the criteria below.

- Design fulfilment through the following:
    - User to capture configurations.
    - Rules to be created based on user configurations.
    - Rules to detect intrusion from a known intrusion set.
    - Rules to detect intrusions irrespective of the number of devices.
    - Determine whether unknown intrusions can be detected; and
    - Notify the user when an intrusion occurs through an alert.

The following are the assumptions of the prototype as per the architecture mentioned in Chapters 2 and 4.

- The smart hub that (a) routes the connection from the external network into the internal network, and (b) routes the connection between the devices, can identify the devices that connect to it; and
- Devices do not communicate directly but rather through the smart hub. Hence, all the connections are known to the smart hub.

A smart hub and six smart home devices were chosen for simulation to verify and validate the correct operation of the proposed NIDS. A client-server architecture was used to verify and determine whether the created user rules correctly identify connection attempts as intrusions.

The smart hub connects all devices and routes their respective connections from the external network to the internal network. A user interface was developed for the smart hub. The local device used to develop the application conformed to security, and the user was authenticated successfully to access the device. Users identify each device within the network by providing a unique name, its triggering device, and the device's triggering method.

User rules (both direct and indirect) are generated through user configurations and known attack signatures are added to the intrusion dataset. The NIDS is configured to monitor the smart home internal network. The prototype components implemented to simulate the smart hub and smart home devices are illustrated in Figure 5.1.

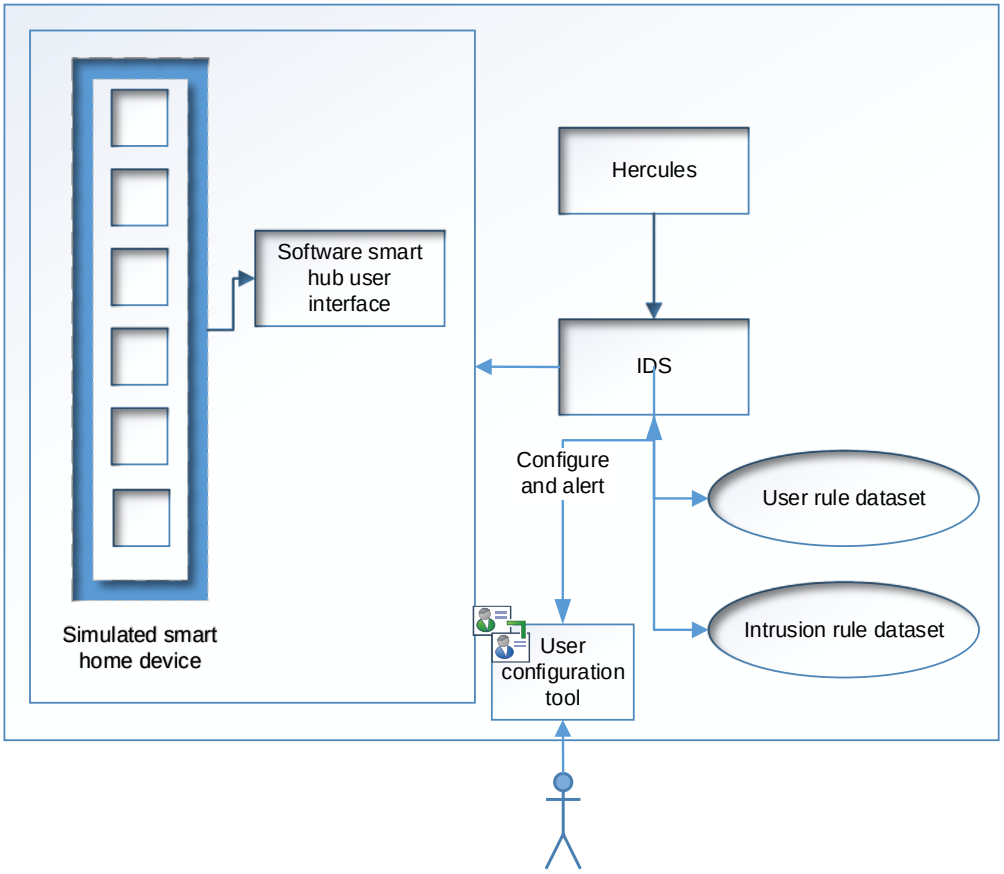


Figure 5.1: Data flow in the prototype

Verification was performed through the following test scenarios:

- Scenario 1: Verify if the user rule set operates as intended to detect unwanted connections between internal smart home IoT devices.
- Scenario 2: Verify if the user rule set operates as intended to detect unwanted connections from the external network.
- Scenario 3: Verify if an attack in the IoT network dataset detects intrusions when connections are sent through; and
- Scenario 4: Verify if a user is alerted when an intrusion occurs.

The section hereafter explains the prototype functionalities.

5.2.1 Prototype functionalities

The prototype mainly needs to showcase the following functionality, which is divided into two main modules, as below and will be detailed in the following sections of the chapter.

- Design that involves user – User configuration and rule creation:
    - User to capture configurations.
    - Connections to be allowed or disallowed based on non-mandatory configurations.
    - Rules to be created based on user configurations; and
    - Dataset of user rules to be created.
- User alerts (making users aware of security breaches) – Intrusion detection module:
    - To check if rules from the IoT intrusion dataset detect intrusions; and
    - Verify if the prototype detects an intrusion into the internal network from a disallowed external network.

5.2.2 Design: User configuration and rule creation

The user should be able to set up user configurations, and direct and indirect rules generated from the user configurations. Direct rules allow the connection, and indirect rules should detect intrusions.

In a real-time system, the smart hub would have identified the smart home devices connecting to it and validated that these devices connect to the same network as the smart hub. The user should be able to capture the user configuration for each device using a very simple scheme. In a real-time system, users may provide a password for all connections or multiple passwords for each connection before approving the connection made.

In the same way, a user interface is developed where the user captures the configurations for each device. Six devices, D1, D2, D3, D4, D5, and D6, have been identified by the smart hub as existing devices in the smart home internal network. The user needs to identify these devices using a name and provide user configurations such as trigger devices and triggering methods.

In the screenshot, Figure 5.2, the user sets up the configurations for how a specific device, D1, should behave. The triggering device prompts the device and initiation method, host ID, which is the MAC address, start time and end time. The start and end time being when the device can have connections set up.

The MAC address and time are non-mandatory fields for a specific device. When the user rule button is clicked, then rules are generated using the mandatory fields and saved to a user rule dataset.

The next screenshot, Figure 5.2, shows where the user can capture configurations in the prototype and dataset generated in Figure 5.3. These configurations address the security challenge of the identification of smart home devices.

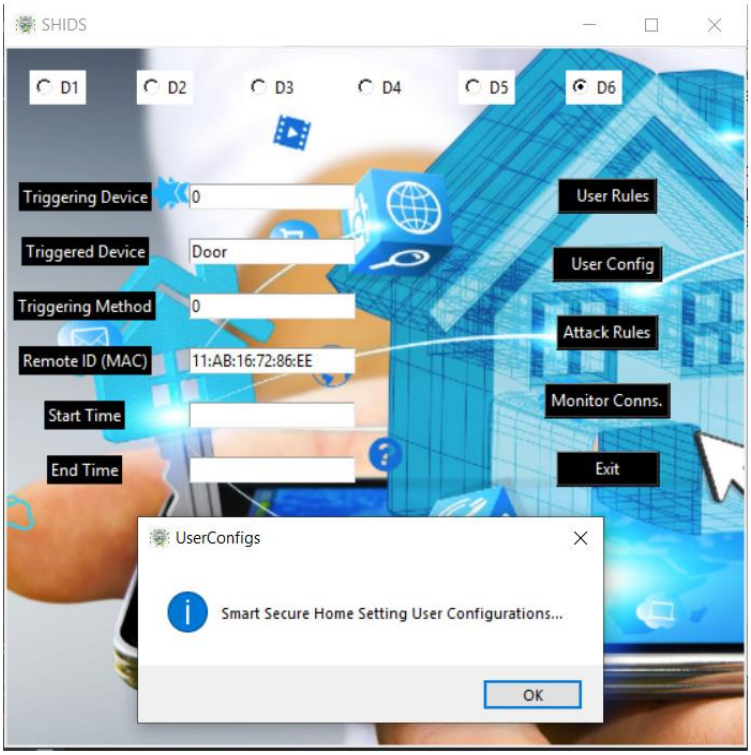


Figure 5.2: User interface application landing page

The actual rules are created at the back end in a user rule dataset file. The NIDS will use these to detect intrusions. When “User Config” is selected on the screen, the configurations from the non-mandatory fields are set to be used while a connection occurs. The sample user rule dataset generated as per configurations is shown in Figure 5.3.

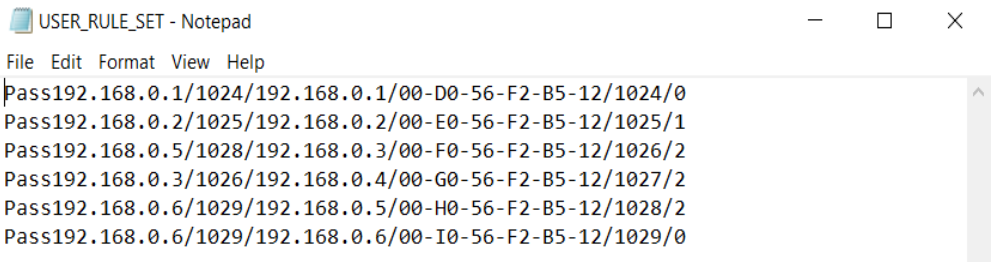


Figure 5.3: Setup of user configuration

Back-end logic is developed to generate the rules for each scenario using the user configurations as in previous explanations in Chapter 4.

When all the configurations have been captured for each device, the intrusion dataset, which are rules from the IoT network dataset of known attack signatures, is subsequently created in a file. A sample of the dataset is shown in Figure 5.4.

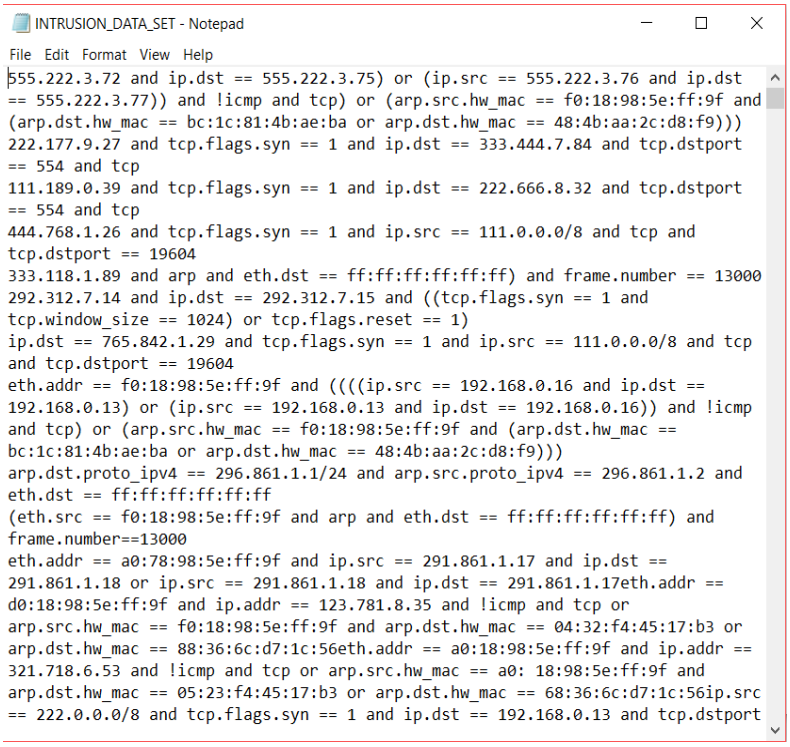


Figure 5.4: Intrusion rule dataset

Once the rules have been created in the datasets represented as files in the prototype, the NIDS starts monitoring connections, which are explained in the next section.

5.2.2 NIDS

Once the NIDS has started monitoring the connections, the client, the smart home device is ready to connect to the smart hub so that the connections from them can be validated against the user configurations and the known intrusion dataset. The client is shown in Figure 5.5, from where the smart home devices are initiated.

Figure 5.5: Page to trigger device connections (internal connections between devices)

The devices are initiated by trying to connect, simulating a real-life scenario. Connections are simulated, and the user identifies each device; for example, “Switch” is used for this purpose. In a real-time environment, connections will be monitored as and when they take place.

When a device is not allowed to connect to another device as per user configurations, the rule generated in the rule set will trigger an intrusion and alert the user through the pop-up screen, as shown in Figure 5.6.

In Figure 5.6, the device “Switch” tries to connect to “Fridge”, which is not part of the automated scenario of the user’s smart home environment and alerts as an intrusion on the user interface. This alert verifies scenarios 1 and 4.

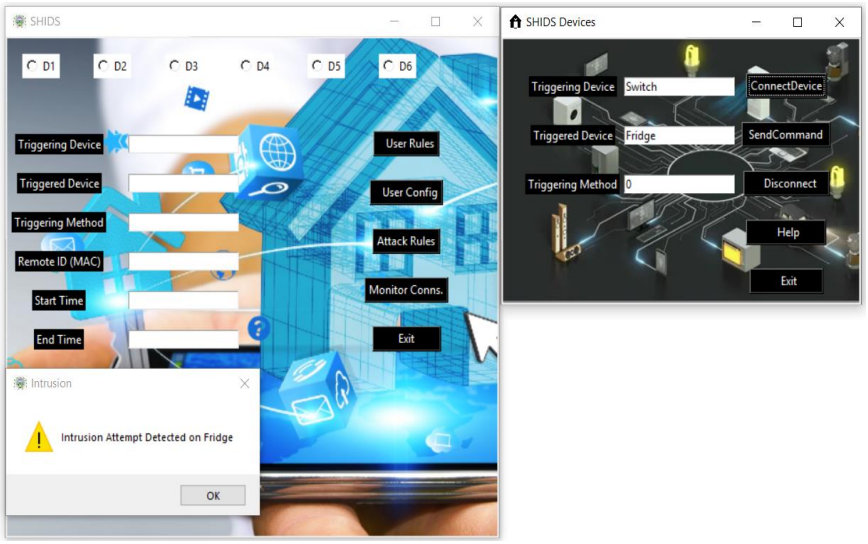


Figure 5.6: The user is alerted of the connection that was an intrusion.

External connections or known intrusions are simulated using the IoT network dataset, which has attack descriptions and is passed through Hercules to the server to determine whether intrusions are detected. The smart hub detects the intrusion and alerts the user. This verifies scenarios 3 and 4.

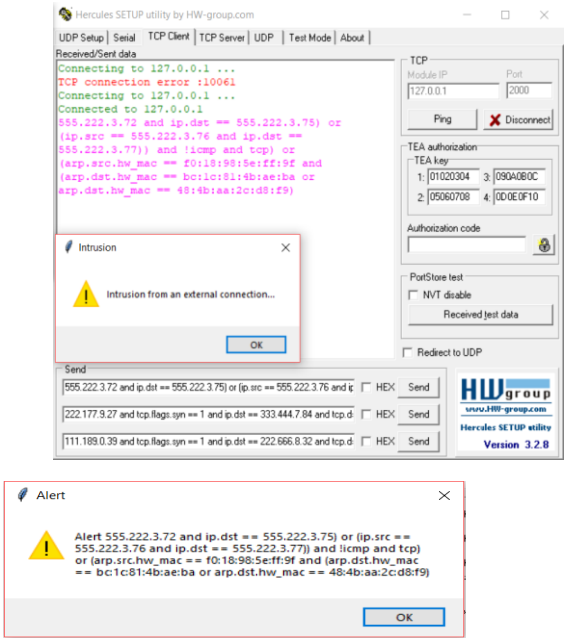


Figure 5.7: Invalid connection from an external connection detected as an intrusion

The prototype was tested to see if intrusions could be detected based on user configurations and the intrusion dataset. These detections verify scenarios 2 and 4.

All internal connections between devices and external connections that should not have taken place as per user configurations were alerted as intrusions. Connections that could take place between devices were not alerted as intrusions. Attacks classified under the IoT network dataset were also detected as intrusions.

All connections made through the NIDS were generated into a file log, captured in Figure 5.8. A technical user can use this further to interpret connections that came through the smart home.

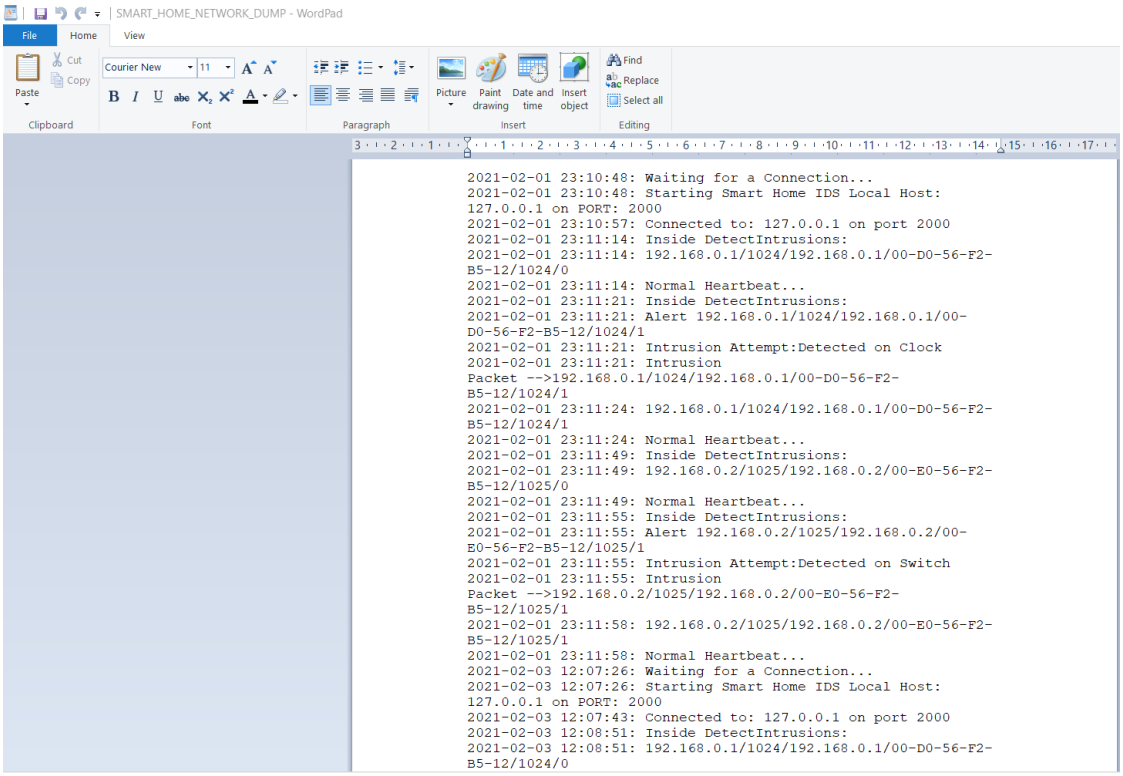


Figure 5.8: Network log

5.3 Conclusion

The chapter discussed a prototype to simulate the proposed design discussed in Chapter 4. Users can use a simple configuration to protect their devices and be aware of any intrusions in their internal smart home network. The user rule dataset consists mainly of rules generated through basic user configurations. The attack signatures or existing intrusion data set were used to detect known attacks. External connections were sent through Hercules to determine if intrusions could be detected. The rules generated from the user configurations proved to detect these intrusions, where the configuration parameters,

such as the trigger device and triggering method played an essential role in detecting intrusions. Additional configurations were also provided for users who prefer additional security for specific devices controlled by the smart hub, which also proved useful in detecting unwanted connections. The configuration can be set up irrespective of the number of users in the network and does not look at specific device profiles to identify these intrusions. The next chapter evaluates the prototype and what has been achieved.

6
Verification and Validation

The developed prototype starts by identifying the devices within a user's smart home environment capturing a set of user configurations from the user to create rules within a smart home internal network. The fact of users being involved, was identified as an important factor to help with security issues in the smart home. The proposed solution developed a design to involve users in identifying intrusions and alerting them, thus making them aware of security breaches within their home. The results and test scenarios of each of the prototype phases are shown in the next section.

6.1 Verification and validation of test results

This section evaluates the prototype. Verification and validation are carried out by providing valid and invalid input to get the expected results. The following steps are required for this:

- Testing methodology
- Test analysis and results

6.1.1 Testing methodology

The research followed an approach based on the waterfall and prototyping model. In conjunction with these approaches, the testing methodology, the V model, is used in this research as it was originally derived from the waterfall model [87]. The model executes testing of the waterfall phases such as requirements, analysis, design, and implementation into different testing phases such as unit testing, integration testing, system testing and acceptance testing. As in the typical waterfall model, the output result will act as the input to the next phase. The model will be executed by testing to see whether the prototype

functions and meets the research goal. Based on the testing model, the test cases are discussed in the next sections.

6.1.2 Test analysis and results

The test analysis will include test cases or test scenarios and test results. The test results show the results of the test cases executed to test the prototype thoroughly. The efficiency of the design developed can be determined by detecting intrusions that occur internally, as well as intrusions that occur from outside the smart home network. The following are the test cases identified to validate the verification scenarios:

- Legitimate connections: These are connections that the user has configured and that may take place, such as allowing one device to trigger another. These should not be considered as an intrusion, neither should an intrusion be triggered, and the user should not be alerted. This helps address the security challenge of identification in access control by identifying the devices within the smart home environment, as well as identifying any external connections other than that within the smart home environment.
- Invalid connections: These are connections that could occur between the devices, but not as per user configurations. These could be an invalid connection taking place, and intrusion should be triggered, and the user should be alerted. These attacks would be classified under unauthorised remote access and would address security challenges such as node trustworthiness in misbehaviour detection and security reporting.
- An attack signature from the IoT dataset is sent via Hercules. These are intrusions to which users should be alerted.
- External connections: These are connections coming from the external network which are not specified and should be detected as intrusions.

6.1.2.1 Test results

The test results are shown in Table 6.1.

Table 6.1: Test Cases and Results

Test case	Test result
Legitimate connections: These are connections that the user has configured, and which may take place. These should not be considered as an intrusion, and the user should not be alerted.	Intrusions were not alerted, and direct rules allowed safe connections. Connections from remote MAC addresses were also specified. Appendix Figures 1, 2, 3, and 4 show proof of results where the user identified the device and connections were made which did not result in intrusions.
Invalid connections: These connections may not take place based on the user configurations. These are intrusions, and the user should be alerted.	Users were alerted, and intrusions were detected using the indirect rules Figure 5.6 in Chapter 4 and Appendix Figure 5 show proof of intrusions alerted
An attack signature from the IoT dataset is sent via Hercules. These are intrusions, and the user should be alerted.	The attack signatures were identified using the IoT network dataset rules. Figure 5.7, Appendix Figures 7 and 8 show proof of intrusions alerted.
External connections were sent via Hercules. These are intrusions and the user should be alerted	The connections were identified as intrusions as shown in the proof in Figure 6.2. The user rule dataset identified these as intrusions as the device was not expecting a connection externally and could not recognise the MAC address identified.

	This also proved that the rules from user rule dataset will first trigger an intrusion if the connection is not meant to happen. The attack rule dataset will only trigger an intrusion if the rule matches the connection being made.

In addition to legitimate connections, a list of invalid connections was made between the devices that triggered intrusions. A list of unknown Hercules intrusions from Hercules was sent through smart home devices to test whether unknown Hercules intrusions that could occur in the future, might be detected. The unknown intrusions were connections from an external IP address that was not present in either the user rule dataset or the intrusion dataset. All intrusions were detected successfully. This is because the indirect rules and the rule syntax, including the triggering method, were derived from the user configurations. Attacks that were meant to be detected were detected using the rules from the intrusion dataset or the user rule dataset. Remote MAC addresses specific to certain devices were also sent through Hercules to that specific device which was allowed and classified as a normal connection as shown in the figure below.

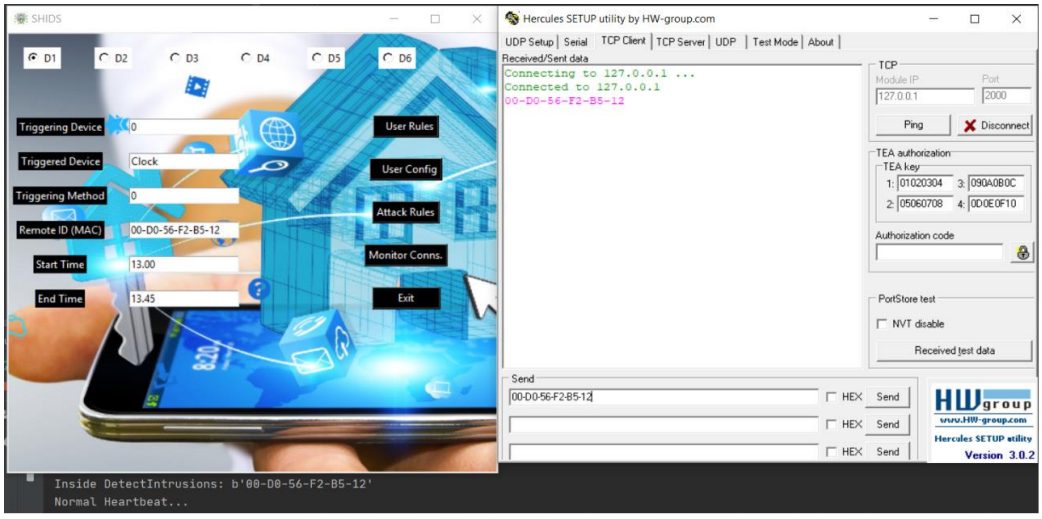


Figure 6.1: Valid connection from MAC address

The same remote MAC address was used to connect to other devices which had no specification of that MAC address in the user configurations, and those were alerted as intrusions as shown in the figure below.

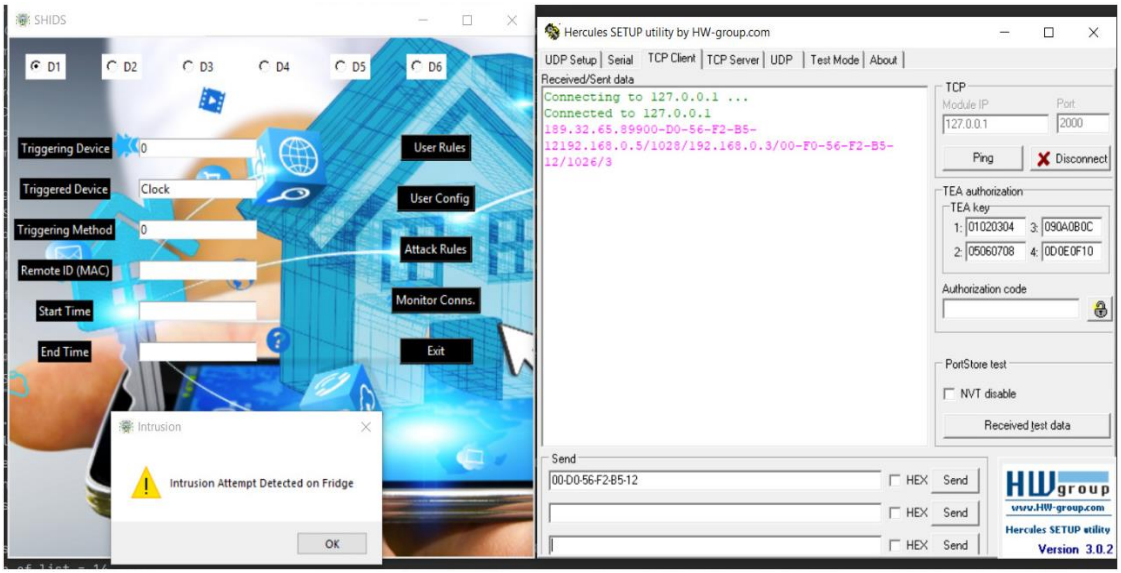


Figure 6.2: Intrusion detected from MAC address where the MAC address was not specified

These validation scenarios proved that the design also helps with the mitigation goal of protecting device security by ensuring that unwanted connections are not made through the NIDS, and consequently help with the mitigation goal of protecting individuals' privacy.

All connections made through the NIDS were generated into a file log as shown, as proof in Figure 5.8 and would help in addressing the challenge of security auditing.

6.1.2.2 Evaluation of the test results

The uniqueness of the prototype lies in the design developed where users are asked to capture how their devices should behave and the configurations and rules formulated accordingly, based on the user configurations. Capturing the user parameter and forming rules based on them is a unique approach that has not been done before to the author's knowledge in the smart home IoT context, to provide and facilitate the extra security that is required at the user level. Moreover, there have been various calls for users to also take responsibility to protect their smart home devices as mentioned in Chapters 1, 2, and 3. The user configurations were not only able to detect known intrusions but also unknown intrusions at devices for connections that did not have a source IP address and

where another device could not trigger it. Users were also alerted when intrusions occurred. Devices that had another device triggering could not detect those unknown intrusions, as the rule formations for such specific devices had source IP addresses defined in them. The ability to make use of user configurations and alert users of intrusions makes users aware, in contrast to what the survey and table highlighted in Chapter 3. The adaptation of the IDS should be evaluated as well, and this is explained in the next section.

6.1.2.3 Evaluation of IDS

The most common measures of IDS evaluation are precision, recall, and F-measure. Precision (P) is the proportion of connections correctly identified as intrusions. Recall (R) measures the proportion of intrusions which were correctly identified amidst the total of all correctly identified intrusions and intrusions that are classified as normal. These two measures are used in the F-measure (F), which calculates the harmonic mean of precision and recall and provides a single weighted metric to evaluate overall performance [19]. These are calculated using the following equations.

$$P = \frac{TP}{TP + FP} \quad (1)$$

Precision Equation

$$R = \frac{TP}{TP + FN} \quad (2)$$

Recall Equation

$$F = 2.\frac{P.R}{P + R} \quad (3)$$

F-measure equation

FP, FN, TP and TN are described in the next section.

False positive (FP): non-intrusive behaviour that is wrongly classified as intrusive by the IDS.

True positive (TP): non-intrusive behaviour that is successfully labelled as non-intrusive by the IDS.

True negative (TN): normal behaviour that is successfully labelled as normal by the IDS.

False negative (FN): Intrusions that are missed by the IDS and classified as normal/non-intrusive.

Performance was tested and compared against that of two smart home environments, where the first smart home environment has user configurations. Therefore, the user configurations, the user rule dataset, and the intrusion dataset were present. The second smart home has no user configuration and hence no user rule dataset and only the intrusion dataset. This was to test the performance of the IDS in detecting intrusions where user configurations are used and/or not used.

A random number of connections were sent through, from which 150 were legitimate connections, 150 were attack signatures that were known and present in the IoT network dataset, and 50 were invalid connections that occurred from external connections. There was no conflict between the user rules and IDS rules; however, more than one rule did detect the same intrusion. The user configuration rules detected invalid intrusions, whereas the attack signatures also detected specific types of attack.

In smart home 1, all the valid connections from the detected user rule dataset detected were 100%. All known intrusions were detected at 100% level, and all external connections sent from external connections were also detected at 100%. Legitimate connections also included remote MAC addresses specified for specific devices that were considered normal. However, 10 external connections were sent from the remote environment to devices, which were not specified and alerted as intrusions. Therefore, the value of precision, recall, and F-measure is as shown in Table 6.2.

Table 6.2: P, R and F measure the results of smart home environment 1

P	R	F-measure
1	1	0.94

In smart home 2, no user configurations were provided and hence no rules generated based on user configurations. Only attack signatures were used. Any valid connections made between the devices were not detected as there were no user configurations. All known intrusions (attack signatures) were detected at 100% and all external connections sent from external connections were also not detected and classified as normal, as there were no rules to identify any external connections occurring on smart home devices. Hence, the value of the measure P, R and F-measure is shown in Table 6.3

Table 6.3: P, R, and F measure the results of smart home environment 2

P	R	F-measure
0.90	0.33	0.49

These indicated that user rule datasets created through user configurations were successful and that just using a predefined intrusion set may not yield the full results of detecting intrusions, unless updated frequently. The user is not aware of any connections that can control their smart home IoT devices, and because there are no user configurations, they are not alerted to any intrusions. This will not bring about user awareness with regard to protecting smart home devices, and the user is unaware of any external connection that takes place with their smart home device that should not be taking place.

It was noted that the non-mandatory field, such as the time for a specific device, did not play a vital role in determining the security, as it just allowed or disallowed connections at that specific time. An intrusion could occur in a device within the time it was active

and where no user configurations were specified. Hence, user configurations and rules generated from them became a critical factor in alerting users.

The specified remote MAC address was helpful, however, if the smart hub was not able to determine the MAC address in the connection, or if the MAC address was not present in the connection or specified for a device: then intrusion was alerted, and false alarms were generated. If the external device of the MAC address, from which the external connection came, was compromised, the smart home environment could be vulnerable and could also be compromised as well. Consequently, it was noted that the specification of an external remote MAC address from which a user may access their smart home device might not be such a good option, for that could provide easy access into the smart home environment for an intruder that had already compromised the device with the unique MAC address.

6.2 Conclusion

This chapter discussed the validation of what was achieved through the prototype. It was noted that all scenarios mentioned in the validation were successful. The prototype proved that users can be involved in configuring their smart home devices using certain parameters. These parameters can be used to detect intrusions occurring on their smart home devices, while noting that real-time intrusions that have caused damage based on examples mentioned in Chapter 2, are intruders connecting from an external network. Although various literature reports have mentioned users presenting a gap in security, with the complexity and difficulty of heterogeneous environments blocking them from finding a holistic solution in addressing these security breaches, the prototype was functional in alerting users when an external connection was made. This research at this time proposes that disconnecting from the internet would be an ideal mitigation strategy as soon as an intrusion is alerted as users are all not technologically savvy. Another mitigation strategy that could be applied is packet filtering where external connections, or connections that are invalid, are not allowed with specific devices. However, the feasibility of this needs an extensive study. This is also due to the heterogeneous environment that smart home environments present, and without proper analysis of each smart home environment device being dealt with, existing security mechanisms within

the smart home environment regarding any other generalised mitigation strategy, may not be successful.

7

Conclusion

This thesis focused mainly on conceptualising a design that involved users by adapting IDSs to address the statement by many authors that users should be responsible for protecting their own smart home devices. The overall result was involving the end users and, through user alerts, making them aware of intrusions surrounding their smart home environment and its devices. This chapter focuses on evaluating the extent to which the objectives of this research study has been achieved, the scope for improvements, and finally, addresses the scope for future research that should be considered.

7.1 Research Synopsis

IoT security and privacy issues are discussed in length, and various research tests have shown the risks associated with them. Smart home devices are targets of these security risks, and there have been many such real-life cases where smart home devices were compromised without the knowledge of the user. Subsequently, trust is such an important factor in these cases, and user security of smart home devices becomes a vital factor. Therefore, it is also vital to detect intrusions that occur in them. In this thesis, a new design involving users was introduced to detect intrusions through user configurations and to create alerts when an intrusion occurs – thus making them aware of security in an internal smart home network. The primary objective of this research was to involve users in setting up their smart home devices and using these user configurations as a base to detect intrusions. In addition, the rules of the IoT network dataset were also used to detect intrusions. To achieve the objective of detecting intrusions, a design was proposed, and a prototype was implemented.

The thesis is constructed in the following format, thus answering the research questions that were presented in Chapter 1.

The thesis began with an introductory chapter that addressed the major issues that IoT currently has and eventually led to the problem statement. In verifying and validating the problem, the dissertation discussed the IoT building blocks, general architecture of IoT, and led the way to smart home architecture. The security issues within the IoT architecture were discussed, describing the different layers within the architecture. It evaluated the layer in which the problem statement fell in Chapter 2 and discussed issues specifically within the smart home vulnerabilities network. This led to the answers to the following research questions: What is the essence of the current IoT architecture, and what kind of security is provided by different service providers? What is the user-level security in the perception layer and application layer in the current IoT architecture? And what methods can be applied in acquiring user security and privacy?

It then followed into the third chapter, evaluating major existing research in the field and just generally around user security. This chapter also evaluated the user-security component in existing research and evaluated methods that can be used. This helped to answer the following research questions: How can user-level security be improved in the application and perception layer in the current IoT architecture, will this really help user security and privacy, and will this answer the first part of the question? What are some of the existing research theories that provide user security, and how do the solutions proposed at the user level, differ?

This led to Chapter 4, which conceptualised a logical design and presented a solution to the problem statement by describing a design that made use of user configurations. Some of these user configurations were mandatory and some were non-mandatory. These mandatory user configurations created rules that detect intrusions. This answered the second part of the research question: What are some of the existing research findings that provide user security and how do the solutions proposed at the user level, differ?

The last question was answered by developing a prototype in Chapter 5 and evaluating it in Chapter 6. It described how data would flow from one component to another and showcased a client-server architecture using user configurations, rule generation, and intrusion detection. It also validated and verified how intrusions are detected in two

different smart home environments where one has user configurations, and the other does not.

The next section explains the achievement of the research goal through the prototype.

7.2 Accomplishing the Research Goal

This section explains the accomplishments of the prototype and hence the attaining of the research goal. The following sections offer a critical evaluation of what this research has achieved.

7.2.1 Achievement of the prototype vs. the problem statement.

The idea of the research is to use user configurations to allow or disallow connections and to create rules that ensure user security in IoT smart home devices; hereby the rules use the user input on how the devices should behave to detect any intrusions occurring in the smart home network. The prototype is developed to showcase the following:

- Developing a design that involves users is possible within a smart home environment where simple user configuration can be used to alert users using smart home devices. These can be achieved by bearing in mind the following:
    - Configurations are simple enough to perform and
    - Applicable to the smart home environment with one or more users, where they are
    - Adapting the IDS functionality and generating rules based on user configurations to detect intrusions.
    - It is important to note that:
        - Certain user configurations, such as time and remote MAC address, may not be useful in security applications or in alerting the user.
        - User configuration such as remote MAC address or even remote IP address may not be 100% effective in allowing connections and may cause false alarms.
    - Incorporating an existing IoT network dataset of known attack signatures to detect existing intrusions, may be useful/recommended.

7.2.2 What makes the proposed design unique?

- Devices are identified by the user providing a unique device name.
- Although the method of creating a rule is the same, the rules generated are very dependent on the user configurations, and hence will be unique to each smart home network. Most of the rule-based systems in IoT concentrate on network-based information and, consequently, rules consist of typical network characteristics. Many research findings including [111, 112] discussed that existing security proposals, including the ones where IDSs are incorporated, have challenges due to the differences in smart home environments. A solution where users are involved has not been proposed thus far and only existing databases have been incorporated to detect intrusions. The importance of users protecting their own devices has been considered by many researchers. This solution proposal, to the author's knowledge, is the first of its kind in the smart home environment that involves users in the rule configuration to detect intrusions.
- All security systems, since they are mostly network-based or device-based, are rule-based systems consisting of attack signatures that need to be fulfilled. The prototype is not only user-based but can detect intrusions based on attack signatures as well.
- Non-mandatory user configurations can allow and disallow connections to a certain extent. However, rule generation seems to be a critical factor in alerting users correctly.
- The user can change any user input at any point in time, and this will generate new rules that are valid and delete the old rules for that specific device.
- The user configurations specified are independent of the number of users in the smart home and independent of the individual devices.

7.3 Future research and limitations

Although the proposed methodology has achieved the objectives described in the previous section, this research still has scope for improvement. The scope of improvement and limitations is explained in the following subsections.

7.3.1 Safeguarding the Smart Hub

The proposed design aims to involve users by using user configurations and alerting users in the smart home where a smart hub is used. The smart hub can be protected using a two-factor authentication; however, this might not be enough to protect the smart hub. Once the smart hub is compromised, the attacker could compromise the smart home environment as well.

Hence, the first and foremost improvement is to protect the smart hub. In the case where an intruder is aware of the smart hub and tries to compromise it, they might try to spoof the smart hub to learn about all the connections. The smart hub should be secured. The system should be designed in such a way that an extra random password is required, or encryption is required to make a connection with the smart hub initially.

7.3.2 Safeguarding smart home devices

Although smart home devices are protected using the user configurations and an intrusion could be alerted, there could be a scenario where an attacker has compromised a device that may not have any user configuration, because they are auto triggered, through another device that can trigger the specific device or even physically tamper with the device.

Any extra security mechanism that can be provided for smart home devices should be provided, especially since the cases of intruders compromising smart home devices are on the rise. Although intrusions may be detected, any kind of prevention should also be implemented. Instead of making the devices discoverable to the external network, one way would be to use network address translation on a smart home network where the devices can use a private IP address and use public IP addresses on the external network.

7.3.3 Improving user configurations

Existing user configurations have been thought of that could alert the user of intrusions and are independent of the number of users within the smart home environment.

The viability of introducing user configurations on devices should be investigated and implemented if possible. This could help in a smart home environment where smart

hubs are not used, and devices are directly connected to the cloud and are functional. The viability of using user configuration on devices could be researched.

All aspects including the number of users in the smart home network, other initiating features of the devices, and the functionality of the devices should be taken into consideration as different protocols and logic within devices could become issues when implementing the same set of user configurations for all devices. However, careful consideration should also be given to using a user input that can generate a false alarm.

7.3.4 Improving mitigation through prevention or reaction

The existing research adapted an IDS to detect intrusions and alert users of intrusions. However, an intrusion prevention system can be adapted in future to mitigate intrusion impact by learning the kind of intrusions associated with smart home environments. Again, a mitigation strategy would have to be devised so that it can be applied to all smart home environments in view of the differences and complexities within the smart home environment. This mitigation strategy will have to be thought through after determining the detection strategy applied in the smart home environments. The research did discuss the possibility of applying a packet filter – this, however, was not implemented, as extensive analysis would be required to understand the infrastructure, device configurations, security, communication technology, etc. within the environment and it would therefore not be possible to say, if it would in fact be a generalised mitigation strategy that would be applicable for all smart home environments.

7.3.5 Improving the intrusion detection rate

The existing research has a detection rate of 0.94 due to false alarms, where the ideal rate would be 1.

Further research can be done to consider what other network details, device details or aspects of an intrusive signature can be taken into consideration to detect an intrusion that would not cause false alarms. Common device information may also be considered to be included in the rules.

The IoT network dataset was incorporated to detect existing IoT intrusions; however, using any kind of existing signature database would mean that these would have to be

continuously updated to ensure the latest attacks are identified. In future, any other signature database could also be potentially incorporated providing that resource capacities within the smart home environment are met.

Machine learning and artificial intelligence techniques may also be introduced to learn about and detect new intrusions, network parameters or connections that may be specific to the smart home environment.

7.3.6 Future improvements to the proposed design

Another future improvement for the design is to enforce the extra authentication mechanism to check once a connection needs to take place between the device and, if possible, configure the smart hub or improve the smart hub; this can occur in such a way that certain details such as authentication, authorisation, unique ID or features specific to that device can be requested for the devices. This can only be accomplished by studying the various types of smart hubs or IoT gateways and their common features in greater detail.

Currently, the IoT network dataset rule is interpreted through a tcpdump tool that interprets the source IP address and uses the IoT network dataset as its intrusion dataset. Many datasets have many different formats, so that one improvement that can be made is to accept and read any form of dataset for intrusion signatures sent to the IDS.

The main limitation of this research would be if an insider intrusion occurs in the following form, i.e., where a user other than the original user who has set up the rule for the device, changes the initial user rules or uses the information such as IP address details to cause an intrusion to the devices in the smart home. Intrusions may occur from a remote MAC address that is specified, which may also be considered as inside intrusions. Unfortunately, inside intrusions have always been a problematic area in the field of security and remain a limitation of this research as well.

The smart hub may not be able to identify the remote MAC address in an external connection, which may also cause false alarms and can also be considered a limitation of this investigation.

The design was implemented within a smart home network that may have a limit to several devices. Therefore, the processing power and speed in determining intrusions will also be determined by the quality of the network within the smart home and is scalable within the smart home networks.

This may be adopted to larger projects such as smart cities, and if high processing servers and databases are provided with good network quality, the same configurations may be considered for other IoT applications where numerous devices are connected. The implementation of this in various other applications is dependent on the nature of the devices used and the external connections that could occur. In IoT applications where external connections should be allowed, user configurations may not be successful due to the number of external connections that could occur and all aspects, such as, which connections can be allowed and should be alerted, so an intrusion would be a major factor in determining the success of it.

The research was intended to provide a design involving the user to determine how their devices should behave. Once the devices have been identified and configurations have been made, the users should be alerted when their devices do not behave. This has been achieved in the research. Although there are areas of improvement and limitations as mentioned above, the research was successful in that it involved users in creating configurations and to use them to detect intrusions and make them aware of intrusions around security in IoT smart home devices. This was made using the induction inference technique which is the inference based on observation through the prototype.

Given the heterogeneous and complex nature of smart home environments, one might find that defining a holistic security solution and generalised mitigation strategy, and using only existing attack signatures to detect intrusions, may not yield a 100% success rate in any given smart home environment. The solutions have to be considered carefully due to the differences, which is why the existing security risk frameworks do not completely cover every aspect of IoT systems. As the number of devices increases, so does the complexity of everything functioning together. It is better to think about first detecting an intrusion at user level, where users are aware of their smart home devices and environment which this research achieves rather than wait for a complete solution where everything works together in a real-life scenario.

References

[1] "ICT facts and figures 2015." ITU. Accessed: Oct. 8, 2021]. Available: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] "Global digital population as of July 2020." Statista. Accessed: Oct. 8, 2021. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/

[3 L. Coetzee and J. Eksteen, "The internet of things – promise for the future? An introduction," in *Proc. 2011 IST-Africa Conf.*, Botswana, May 2011, [Online]. Available: http://ieeexplore.ieee.org/document/6107386/.

[4] H. Kim, H. Chang, J. Suh and T. Shon, "A study on device security in IoT convergence," *Proc. Ind. Eng. Manage. Appl. (. ICIMSA)*. South Korea, Jul. 2016, [Online]. Available: http://ieeexplore.ieee.org/document/7503989/?section=abstract

[5] M. Nallapaneni, M. Kumara and K. Mallick, "The Internet of Things: insights into the building blocks, component interactions, and architecture layers," in *Int. Conf. Comp. Intell. Data & Data Sci.(ICCIDS)* in Procedia Computer Science, 2018, pp. 109–117. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050918309049

[6] M. J. Chin and A. Winckles, "Holistic blockchain approach to foster trust, privacy and security in IoT based ambient assisted living environment," in *15th Int. Conf. Intell. Environ (IE),* 2019, pp. 52-55, [Online]. doi:10.1109/IE.2019.00008.

[7] Q. Yue, "Research on smart city development and Internet of Things industry innovation in the "internet +" era," 2021, *3rd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA),* 2021, pp. 28-31, doi:10.1109/ICIRCA51532.2021.9545028.

[8] Z. A. Almusaylim and N. Zaman, "A review on smart home present state and challenges: Linked to context-awareness Internet of Things (IoT)", *Wireless Network*, vol. 25, no. 6, pp. 3193-3204, 2019.

[9] ITU-TY.4806, "Internet of things and smart cities and communities – Identification and security," *Series-Y, Global Information Infrastructure, Internet Protocol Aspects,*

Next Generation Networks, Internet of Things and Smart Cities, Telecommunication Standardization sector of ITU, Nov. 2017.

[10]ITU-TY.4000, "Internet of Things use cases," *Series-Y, Global Information Infrastructure, Internet Protocol Aspects, Next Generation Networks, Internet of Things and Smart Cities, Telecommunication Standardization sector of ITU*, Dec. 2018

[11] ITU-TY.4115, "Reference architecture for IoT device capability exposure," *Series-Y, Global Information Infrastructure, Internet Protocol Aspects, Next Generation Networks, Internet of Things and Smart Cities, Telecommunication Standardization sector of ITU*, Apr. 2017

[12] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," Computer *Networks: Int. J. Comp. Telecomm. Netw. Networking*, vol. 54, no. 15, Oct. 2010, pp. 2787-2805, [Online]. Available: www.elsevier.com/locate/comnet

[13] A. A. Bouaouad, C. S. Assoul and N. Souissi, "The key layers of IoT architecture," in *2020 5th Int. Conf. Cloud Comp. AI: Technol. Appl. (CloudTech)*, pp. 1-4, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/9365919

[14] R. Williams, E. McMahon, S. Samtani, M. Patton and H. Chen, "Identifying vulnerabilities of consumer Internet of Things (IoT) devices: A scalable approach," in *2017 IEEE Int. Conf. Intell. Sec. Inform (ISI)*, pp. 179-181, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8004904

[15] G. Kavallieratos, V. Gkioulos and S. K. Katsikas, "Threat analysis in dynamic environments: the case of the smart home", in *15th Int. Conf. Distr. Comp. Sensor Syst. (DCOSS)*, 2019, pp. 234-240, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/8804734

[16] A. Hameed and A. Alomary, "Security issues in IoT: a survey," in *2019 Int. Conf. 3ICT*, pp. 1-5, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/8910320

[17] J. Shams, N. A. G. Arachchilage and J. M. Such, "Vision: why Johnny can't configure smart home? A behavioural framework for smart home privacy configuration," *in 2020 IEEE Eur. Symp. Secur. Priv. Workshops (EuroS&PW)*, pp. 184-189, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/9229770

[18] N. M. Allifah and I. A. Zualkernan, "Ranking security of IoT-based smart home consumer devices," *IEEE Access*, vol. 10, 2022, pp. 18352-18369, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=9698229

[19] B. D. Davis, J. C. Mason and M. Anwar, "Vulnerability studies and security postures of IoT devices: a smart home case study," *IEEE IoT J.*, vol. 7, no. 10, Oct. 2020, pp. 10102-10110, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/9050664

[20] C. Kolias, A. Stavrou, J. Voas, I. Bojanova and R. Kuhn, "Learning Internet-of-Things security "hands-on"," *IEEE Security & Privacy*, vol. 14, no. 1, Feb. 2016, pp. 37-46, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/7397713

[21] M. T. Dlamini, M. M. Eloff and J. H. P. Eloff, "Internet of Things: emerging and future scenarios from an information security perspective," in *Proc. SATNAC 2009: Convergence – 21st Century Lifestyle Enabler*, Sep. 2009, pp 1-6. [Online]. Available: https://researchspace.csir.co.za/dspace/handle/10204/4411.

[22] T. Alladi, V. Chomala, B. Sikdar and K. K. R. Cho, "Consumer IoT: security vulnerability case studies and solutions," *IEEE Cons. Electr. Mag.*, vol. 9, no. 2, Feb. 2020, pp. 17-25, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/8977812

[23] R. Yu, X. Zhang and M. Zhang, "Smart home security analysis system based on the Internet of Things," in *2021 IEEE 2nd Int. Conf. Big Data, AI, IoT Eng. (ICBAIE*), 2021, pp. 596-599, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/9389849

[24] W. Iqbal, H. A.M. Daneshmand, B.R. and Y. A. Bangash, “An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security,” *IEEE IoT J.* , vol. 7, no. 10, Oct. 2020, pp. 10250-10276, [Online]. Available: https://ieeexplore-ieeeorg.nwulib.nwu.ac.za/document/9099839/references#references

[25] M. Gajewski, J. M. Batalla, and G. Mastorakis et al. “A distributed IDS architecture model for Smart Home systems,” *Cluster Comput. 22,* Suppl. 1, 2019, pp. 1739–1749 [Online]. Available: https://link.springer.com/article/10.1007/s10586-017-1105-z

[26] Y. Oren and A. D. Keromytis, “From the aether to the ethernet–attacking the Internet using broadcast digital television,” in *Proc. 23rd USENIX Secur. Symp*., San Diego, 2014, pp. 353–368, [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-oren.pdf

[27] S. Chawla and G. Thamilarasu, “Security as a service: real-time intrusion detection in Internet of Things,” in *CyberSec 18: Proc. 5th Cybersecur. Symp.,* USA, April 2018, pp. 1–4, [Online]. Available: https://dl.acm.org/doi/10.1145/3212687.3212872

[28] A. Bryman, “Integrating quantitative and qualitative research: how is it done?”, *Qualitative Research*, vol. 6(1), Copyright SAGE Publications, London, 2006, pp. 97–113, [Online]. Available: https://people.utm.my/uzairiah/wp-content/blogs.dir/1541/files/2016/11/Qualitative-Research-2006-Bryman-97-113.pdf

[29] A. S. Fischler, “Quantitative research methods”, Nova Southeastern University School of Education, 2015, [Online]. Available: http://education.nova.edu/Resources/uploads/app/35/files/arc_doc/quantitative_research_methods.pdf

[30] R. Porkodi and V. Bhuvaneswari, “The Internet of Things (IoT) applications and communication enabling technology standards: an overview,” in *2014 Int. Conf. on Intel. Comp. App.,* pp. 324-329, [Online]. Available: https://ieeexplore.ieee.org/document/6965065

[31] “Vodafone IoT Barometer 2017/2018”, Sep., Vodafone, 2018, [Online]. Available: https://www.vodafone.com/business/news-and-insights/press-release/vodafone-research-reveals-number-of-large-scale-iot-projects-doubled-in-the-last-year

[32] M. H. Asghar, A. Negi and N. Mohammadzadeh, "Principle application and vision in Internet of Things (IoT)," in *Int. Conf. Comp., Comm. & Autom.,* 2015, pp. 427-431 [Online]. Available: https://ieeexplore.ieee.org/document/7148413/metrics#metrics

[33] ITU-TY.2060, “Infrastructure internet protocol aspects and next generation networks,” *Series-Y, Global Information Infrastructure, Internet Protocol Aspects, Next Generation Networks, Internet of Things and Smart Cities, Telecommunication Standardization sector of ITU*, Apr. 2017

[34] S. A. Refaey and A. Shami, "Securing smart home networks with software-defined perimeter," in *15th Inter. Wireless Comm. & Mob. Comp. Conf. (IWCMC),* 2019, pp. 1989-1993, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/8766686

[35] W. Lv, F. Meng, C. Zhang, Y. Lv, N. Cao and J. Jiang, "A General Architecture of IoT System," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, 2017, pp. 659-664, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/8005876

[36] B. Muhammad, R. A. Rehman, B. Khan and B.S. Kim. "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey" *Sensors*, vol. 18, no. 9, 2018, [Online].Available: https://www.researchgate.net/publication/327272757_IoT_Elements_Layered_Architectures_and_Security_Issues_A_Comprehensive_Survey

[37] Z. Zhang, M. C. Y. Cho, C. Wang, C. Hsu, C. Chen and S. Shieh, "IoT security: ongoing challenges and research opportunities," in *2014 IEEE 7th Int. Conf. Service-Oriented Comp. & Appl.*, 2014, pp. 230-234, [Online]. Available: https://ieeexplore.ieee.org/document/6978614

[38] A. Majeed, A. U. Haq, A. Jamal, R. Bhana, F. Banigo and S. Baadel, "Internet of everything (IoE) exploiting organisational inside threats: Global network of smart devices (GNSD)," in *2016 IEEE Int. Symp. Sys. Eng. (ISSE)*, 2016, pp. 1-7, [Online]. Available: https://ieeexplore.ieee.org/document/7753152

[39] J. M. Khurpade, D. Rao and P. D. Sanghavi, "A Survey on IOT and 5G network," in *2018 Int. Conf. on Smart City and Emer. Tech. (ICSCET)*, 2018, pp. 1-3, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/8537340

[40] A. Banafa, "Three major challenges facing IoT," Mar. 2017, [Online]. Available: h/ttps://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html

[41] J. Voas, *"*Networks of 'things*'*," IEEE, 2016, [Online]. Available: https://iot.ieee.org/images/files/pdf/networks-of-things_jeff-voas_5-31-2016.pdf

[42] CL. Zhong, Z. Zhu and R. Huang, "Study on the IOT architecture and access technology," in *16th Int. Symp. Distrib. Comp. Appl. Bus., Eng. Sci. (DCABES)*, 2017, pp. 113-116, [Online]. Available: https://ieeexplore.ieee.org/document/8253048

[43] H. Verma and K. Chahal, "A review on security problems and measures of Internet of Things," in *2017 Int. Conf. Intell. Comp. and Ctrl. Sys. (ICICCS)*, 2017, pp. 71-76 [Online]. Available: https://ieeexplore.ieee.org/document/8250560

[44] S. N. Swamy, D. Jadhav and N. Kulkarni, "Security threats in the application layer in IOT applications," in *2017 Int. Conf. I-SMAC (IoT in Social, Mob., Anal. and Cloud) (I-SMAC)*, 2017, pp. 477-480, [Online]. Available: https://ieeexplore.ieee.org/document/8058395

[45] M. Frustaci, P. Pace, G. Aloi and G. F. Dimes, "Evaluating critical security issues of the IoT world: present and future challenges*," IEEE IoT J.* , vol. 5, no. 4, Aug. 2018, pp. 2483 –2495, [Online]. Available: https://ieeexplore.ieee.org/document/8086136

[46] A. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *52nd ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, 2015, pp. 1-6, [Online]. Available: https://ieeexplore.ieee.org/document/7167238

[47] G. Sharma, N. Pandey, I. Hussain and S. K. Kathri, "Design of framework and analysis of Internet of things at data link layer," in *2nd Int. Conf. on Telecomm. Netw. (TEL-NET)*, 2017, pp. 1-4, [Online]. Available: https://ieeexplore.ieee.org/document/8343520

[48] T. Kim, H. Lee, and Y. Chung, "Advanced universal remote controller for home automation and security," *IEEE Trans. Cons. Electron.*, vol. 56, no. 4, 2010, pp. 2537-2542, [Online]. Available: https://ieeexplore.ieee.org/document/5681138

[49] C. Suh and Y. Ko, "Design and implementation of intelligent home control systems based on active sensor networks," *IEEE Trans. Cons. Electr.,* vol. 54, no.3, 2008, pp. 1177-1184, [Online]. Available: https://ieeexplore.ieee.org/document/4637604

[50] G. Song, K. Yin, Y. Zhou and X. Cheng, "A surveillance robot with hopping capabilities for home security," *IEEE Trans. Cons. Electron.*, vol. 55, no. 4, 2009, pp. 2034-2039, [Online]. Available: https://ieeexplore.ieee.org/document/5373766

[51] S. Raza, H. Shafagh, K. Hewagem, R. and H. T. Voigt, "Lithe: lightweight secure CoAP for the Internet of Things," *IEEE Sensors J.*, vol.13, no. 10, 2013, pp. 3711-3720, [Online]. Available: https://ieeexplore.ieee.org/document/6576185

[52] S. Vashi, J. Ram, J. Modi, S. Verma and C. Prakash "Internet of Things (IoT): a vision, architectural elements, and security issues*," In Proc. 2017 Int. Conf. on I-SMAC (IoT in Social, Mob., Anal. and Cloud) (I-SMAC),* India, 2017, pp. 492-496. [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8058399

[53] M. M. Pillai, J.H. P. Eloff and H. S. Venter, "An approach to implement a network intrusion detection system using genetic algorithms," In *Proc. 2004 ann. Res. Conf. S.A. Inst. Comp. Scientists & Inf. Technol. IT Res. Dev. Countries (SAICSIT)*, South Africa, Oct. 2004. [Online]. Available: https://dl.acm.org/citation.cfm?id=1035080

[54] H. Rahman and R. Rahmani, "Enabling distributed intelligence assisted future internet of things controller (FITC)," *Appl. Comp. Inf.*, vol. 14, no. 1, 2018, pp. 73-87,

[Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210832717300364

[55] M. Sultan and K. N. Ahmed, “SLASH: self-learning and adaptive smart home framework by integrating IoT with Big Data analytics,” in *Proc. 2017 Comp. Conf.*, London, Jul. 2017, pp. 530-538, [Online]. Available: https://ieeexplore-ieeeorg.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8252147&tag=1

[56] T. Perumal, S. K. Datta and C. Bonnet, “IoT device management framework for smart home scenarios,” in *Proc. 2015 IEEE 4th Glob. Conf. Cons. Electr. (GCCE)*, Japan, Oct. 2015, pp. 54-55, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=7398711

[57] L. Liu, C. Zhang and Y. Fang, “EPIC: A differential privacy framework to defend smart homes against internet traffic analysis,” *IEEE IoT J.*, vol. 5 , no. 2, April 2018, pp. 1206-1217, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8278156

[58] W. Li, T. Logenthiran, V. L. Phan and W. L. Woo, “IoT based self-learning home management system (SHMS) for Singapore,” *IEEE IoT J.*, vol. 5, no. 3, Jun. 2018, pp. 2212-2219 [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8340755

[59] J. Chauhan, Y. Hu, A. Misra, A. Seneviratne and Y. Lee, “Breathing-based authentication on resource-constrained IoT devices using recurrent neural networks,” *Computer*, vol. 51, no. 5, May 2018, pp. 60-67. [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8364655

[60] P. J. Rani, J. Bakthakumar, B. P. Kumaar, U. P. Kumaar and S. Kumar, "Voice controlled home automation system using Natural Language Processing (NLP) and Internet of Things (IoT)," *2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM)*, 2017, pp. 368-373 [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8261311

[61] I. Sharma, C. Cañizares and K. Bhattacharya, "Residential micro-hub load model using neural network," *2015 North American Power Symposium (NAPS)*, 2015, pp. 1-6, [Online]. Available:https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=7335091

[62] C.C. Teoh and C.E. Tan, "A neural network approach towards reinforcing smart home security," in *Proc. 8th Asia-Pacific Symp. Info. Telecom. Tech.*, Malaysia, Jun. 2010, pp. 1-5, [Online]. Available: https://ieeexplore.ieee.org/document/5532066

[63] H. D. Mehr, H. Polat and A. Cetin, "Resident activity recognition in smart homes by using artificial neural networks," in *Proc. 2016 4th Int. Istanbul Smart Grid Cong. Fair (ICSG)*, Turkey, Apr.2016, pp 1-5, [Online]. Available: https://ieeexplore.ieee.org/document/7492428

[64] H. Fang and L. He, "BP neural network for human activity recognition in smart home," in Proc. Int. Conf. on Comp. Sci. Service Sys., China, Aug. 2012, pp. 1034-1037, [Online]. Available: https://ieeexplore.ieee.org/document/6394500

[65] S. Choi, E. Kim and S. Oh, "Human behavior prediction for smart homes using deep learning," in *Proc. 2013 IEEE RO-MAN*, South Korea, Aug. 2013, pp. 173-179, [Online]. Available: https://ieeexplore.ieee.org/document/6628440

[66] M.C. Chan, C.P. Hariton, P. Ringeard and E. Campo, "Smart house automation system for the elderly and the disabled," in *Proc. 1995 IEEE Int. Conf. on Systems, Man and Cybern. Intel. Sys. 21st Century*, Canada, Oct. 1995, pp. 1586-1589, [Online]. Available: https://ieeexplore.ieee.org/document/537998

[67] S. M. Brundha, P. Lakshmi and S. Santhanalakshmi, "Home automation in client-server approach with user notification along with efficient security alerting system," in *Proc. 2017 Int. Conf. Smart Tech. Smart Nation (SmartTechCon)*, India, Aug. 2017. pp. 596-601, [Online]. Available: https://ieeexplore.ieee.org/document/8358441

[68] M. L. Ravi, B. Chandra, V. Kumar and B. Suresh Babu, "IoT enabled home with smart security," in *Proc. 2017 Int. Conf. Energy, Comms., Data Analytics, Soft Computing (ICECDS)*, India, Aug. 2017, pp. 1193-1197, [Online]. Available: https://ieeexplore.ieee.org/document/8389630

[69] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *2015 Int. Symp. Cons. Electr. (ISCE)*, pp. 1-2, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/7177843

[70] P. Kumar and U. C. Pati, "IoT based monitoring and control of appliances for smart home," in *Proc. 2016 IEEE Int. Conf. Recent Trends in Elect., Info. Comm. Tech. (RTEICT)*, India, May 2016, pp. 1145-1150, [Online]. Available: https://ieeexplore.ieee.org/document/7808011

[71] Z. Yan, P. Zhang and A. V. Vasilakos, "A survey on Trust management for Internet of Things," *J. Netw. and Comp. Appl.*, vol. 42, pp 120-134, Jun. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1084804514000575

[72] A. Wilde, O. Ojuroye and R. Torah, "Prototyping a voice controlled smart home hub wirelessly integrated with a wearable device," in *Proc. 2015 9th Int. Conf. Sensing Tech. (ICST)*, New Zealand, Dec, pp. 71-75 [Online]. Available: https://ieeexplore.ieee.org/document/7438367

[73] J. H. Han, Y. Jeon and J. Kim, "Security considerations for secure and trustworthy smart home system in the IoT environment," in *2015 Int. Conf. on Info. Comm. Tech. Convergence (ICTC)*, pp. 1116-1118, doi:10.1109/ICTC.2015.7354752. https://ieeexplore-ieee-org.nwulib.nwu.ac.za/document/7354752

[74] I. Del Pozo and D. Cangrejo, "Creating smart environments: Analysis of improving security on smart homes," in *Prc. 2018 IEEE 6th Int. Conf. Future IoT and Cloud (FiCloud)*, Spain, Aug. 2018, 303-310 [Online]. Available: https://ieeexplore.ieee.org/document/8458028

[75] J. Bugeja, A. Jacobsson, and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," in *Proc. 2016 Eur. Inte. Sec. Inform. Conf. (EISIC)*, Sweden, Aug. 2016, pp. 172-175, [Online]. Available: https://ieeexplore.ieee.org/document/7870217

[76] A. Jacobsson, M. Boldt, and B. Carlsson, "A risk analysis of a smart home automation system," *Future Gen. Comp. Sys.*, vol. 56, Mar 2016, pp. 719–733, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X15002812

[77] P. Kumar, A. Gurtov, J. Iinatti , M. Ylianttila and M. Sain, “Lightweight and secure session-key establishment scheme in smart home environments,” IEEE Sensors Journal, Vol.16 , Jan.2016, pp. 254-264, [Online]. Available: https://ieeexplore.ieee.org/document/7234863

[78] S. Rehman and V. Gruhn, “An approach to secure smart homes in cyber physical systems/Internet-of-Things,” in *Proc. 2018 5th Int. Conf. Softw. Defined Sys. (SDS)*, Spain, April 2018, pp. 126-129, [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8370433

[79] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, A. Zanella, “IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices,” *IEEE IoT J.* vol. 6, no. 5, pp. 8182 –8201, Oct. 2019 [Online]. Available: https://ieeexplore-ieee-org.nwulib.nwu.ac.za/stamp/stamp.jsp?tp=&arnumber=8796409

[80] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conf. IoT Soc., Mob., Anal. and Cloud) (I-SMAC)*, 2017, pp. 32-37, [Online]. Available: https://ieeexplore.ieee.org/document/8058363

[81] S. Zheng, N. Apthorpe, M. Chetty and N. Feamster, “User Perceptions of Smart Home IoT Privacy,” in *Proc. ACM Hum. -Comput. Interact. 2, CSCW*, vol. 200, Nov. 2018, pp 1–20, [Online]. Available: https://dl.acm.org/doi/10.1145/3274469

[82] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda and Y. Kato, “Anomaly detection for smart home based on user behavior,” in *Prc. 2019 IEEE Int. Conf. Cons. Elec. (ICCE)*, USA, May. 2020, pp. 183-192, [Online]. Available: https://ieeexplore.ieee.org/document/8661976

[83] “Install PyCharm”, Jetbrains, 2020, [Online]. Available: [https://www.jetbrains.com/help/pycharm/installation-guide.html]

[84] “Building your first python gui application with tkinter”, Real Python, 2020, [Online]. Available: [https://realpython.com/python-gui-tkinter/#building-your-first-python-gui-application-with-tkinter]

[85] “Hercules setup utility”, HW-Group, 2011, [Online]. Available: http://www.hw-group.com/products/hercules/index_en.html.

[86] L. Sadineni, E. S. Pilli and R. B. Battula, "Ready-IoT: A Novel Forensic Readiness Model for Internet of Things," *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, 2021, pp. 89-94, [Online]. Available: https://ieeexplore.ieee.org/document/9595902

[87] “V-Model (Software Development)”, Wikipedia, 2011, [Online]. Available: http://en.wikipedia.org/wiki/V-Model_(software_development).

[88] H. Kang, D. Hyun, A. G. M. Lee, J. D. Yoo, K. H. Park and H. K. Kim, “IoT Network Intrusion Dataset”, IEEE, Sep. 2019, https://ieee-dataport.org/open-access/iot-network-intrusion-dataset

[89] V. Jain and M. Agrawal, “Applying genetic algorithm in intrusion detection system of IoT Applications,” *Proc. 4th Int. Conf. Trends Electr. Inform. (ICOEI*), 2020, pp. 284-287 [Online]. Available: https://ieeexplore.ieee.org/document/9143019

[90]“Structured system analysis and design”, 2020, [Online]. Available: https://en.wikipedia.org/wiki/Structured_systems_analysis_and_design_method

[91] H. Aftab, K. Gilani, J. Lee, L. Nkenyereye, S. Jeong, and J. Song, “Analysis of identifiers in IoT platforms”, *Dig. Comms. Netw.* vol. 6, no. 3, 2020, pp. 333-340, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864818300671

[92] R. H. Member, G. Loukas, A. Bezemskij, and E. Panaousis, “Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning”, *IEEE Transactions Info. Foren. and Sec.* vol. 16, Dec. 2020, pp. 1720–1735, [Online]. Available: https://ieeexplore.ieee.org/document/9277640

[93] M. Gajewski, J.M. Batalla, G. Mastorakis et al. “A distributed IDS architecture model for Smart Home systems,” *Cluster Comput*. Vol. 22, pp. 1739–1749, 2019. [Online]. Available: https://link.springer.com/article/10.1007/s10586-017-1105-z

[94] I. Andrea, C. Chrysostomou, G. Hadjichristofi, “Internet of Things: Security vulnerabilities and challenges,” Proceedings of the 2015 IEEE Symposium on Computers and Communication (ISCC), Cyprus, Feb. 2016, pp. 180-187 [Online]. Available: https://ieeexplore.ieee.org/document/7405513

[95] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” IEEE Access, Volume 7, June 2019, pp. 82721-82724, [Online]. Available: https://ieeexplore.ieee.org/document/8742551

[96] E. Anthi, L. Williams, M. Słowinska, G. Theodorakopoulos, and P. Burnap, “A supervised intrusion detection system for smart home IoT devices,” *IEEE IoT J.*, vol. 6, no. 5, Oct. 2019, pp. 9042-9053 [Online]. Available: https://ieeexplore.ieee.org/document/8753563

[97] M. Nobakht, V. Sivaraman, and R. Boreli, “A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow,” in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Aug. 2016, pp. 147–156. [Online]. Available: https://ieeexplore.ieee.org/document/7784565

[98] A. Procopiou, N. Komninos and C. Douligeris, “For Chaos: Real time application DDoS detection using forecasting and chaos theory in smart home IoT network,” *Wireless Comm. Mob. Comput.*, vol. 2019, Feb. 2019, pp. 1–14, [Online]. Available: https://dl.acm.org/doi/10.1155/2019/8469410

[99] M. Novák, M. Biňas and F. Jakab, "Unobtrusive anomaly detection in presence of elderly in a smart-home environment," *2012 ELEKTRO*, 2012, pp. 341-344, [Online]. Available: https://ieeexplore.ieee.org/document/6225617

[100] S. Ramapatruni, S. N. Narayanan, S. Mittal, A. Joshi, and K. Joshi, “Anomaly detection models for smart home security,” Proc. 2019 IEEE 5th Int. Conf. on Big Data security on Cloud (BigDataSecurity), May 2019, pp. 27-29, [Online]. Available: https://ieeexplore.ieee.org/document/8819458

[101] Z. N. Mohammad, F. Farha, A. O. M. Abuassba, S. Yang and F. Zhou, "Access control and authorization in smart homes: A survey," *Tsinghua Science and Technology*,

vol. 26, no. 6, Dec. 2021, pp. 906-917, [Online] Available: https://ieeexplore.ieee.org/document/9449335

[102] J. Arshad , M. A. Azad, M. M. Abdellatif , M. H. U. Rehman , K. Salah, "COLIDE: a collaborative intrusion detection framework for Internet of Things," *IET Networks*, vol. 8, no. 1, 2019, pp. 12-17, [Online]. Available: https://ieeexplore.ieee.org/document/8355434

[103] O. Lourme and M. Hauspie, "Toward a realistic Intrusion Detection System dedicated to smart-home environments," *2021 17th Int. Conf. Wireless Mob. Comp., Netw. and Comms. (WiMob)*, 2021, pp. 80-85, [Online]. Available: https://ieeexplore.ieee.org/document/9606337

[104] K. Karimi and S. Krit, "Smart home-smartphone systems: threats, security requirements and open research challenges," *2019 Int. Conf. Comp. Sci. Renew. Energ. (ICCSRE)*, 2019, pp. 1-5, [Online] Available: https://ieeexplore.ieee.org/document/8807756

[105] K. Boeckl, M. Fagan, W. Fisher, N. Lefkovitz, K. N. Megas, E. Nadeau, D. G. O'Rourke, B. Piccarreta and K. Scarfone, "Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks", NISTIR, vol. 8228, 2019, [Online] Available: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

[106] "Internet of Things security for small and medium organizations (ITSAP.00.012)", Canadian Centre for Cyber Security, 2019, [Online]. Available: https://cyber.gc.ca/sites/default/files/publications/ITSAP.00.012-en.pdf

[107] "Cyber Security for Consumer Internet of Things: Baseline Requirements", *European Telecommunications Standards Institute, ETSI EN 303 645 V2.1.1*, 2020, [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[108] M. Fahmideh, A. Ahmad, A. Behnaz, J. Grundy and W. Susilo, "Software Engineering for Internet of Things: The Practitioners' Perspective," in *IEEE*

Transactions on Software Engineering, vol. 48, no. 8, Aug. 2022, pp. 2857-2878, [Online]. Available: https://ieeexplore.ieee.org/document/9398558

[109] M. I. Mohamed Ariff, N. K. Hanum Kamaruzzaman, E. I. Zulkiflie, F. D. Mohamad Fadzir, K. A. Salleh and N. I. Arshad, "Design and Development for Smart Home via IoT Technology: A Work in Progress," in *2021 7th Int. Conf. Research and Innovation in Info. Sys. (ICRIIS)*, 2021, pp. 1-4, [Online], Available: https://ieeexplore.ieee.org/document/9617066

[110] N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," *IEEE Access*, vol. 9, 2021, pp. 121975-121995, [Online]. Available: https://ieeexplore.ieee.org/document/9528421

[111] J. R. Saura, D. Palacios-Marqués and D. Ribeiro-Sorian , "Using data mining techniques to explore security issues in smart living," *Computer Communications*, vol. 179, pp. 285–295, 2021, [Online]. Available: https://doi.org/10.1016/j.comcom.2021.08.021

[112] B. Hammi, S. Zeadally, R. Khatoun, J. Nebhen, "Survey on smart homes: vulnerabilities, risks, and countermeasures," *Computers & Security* vol. 117, 2022, [Online]. Available: https://doi.org/10.1016/j.cose.2022.102677

[113] A. E. Omolara, A. Abdullatif, O. I. Abiodun, M. Alawida, A. Alabdulatif, W. H. Alshoura, H. Arshad, "The internet of things security: A survey encompassing unexplored areas and new insights," *Computers & Security*, vol. 112, 2022, pp. 102494, [Online]. Available: https://doi.org/10.1016/j.cose.2022.102677

[114] P. Bhoyar, P. Sahare, S. B. Dhok, R. B. Deshmukh, "Communication technologies and security challenges for internet of things: A comprehensive review," *Int. J. Electron. Commun. (AEÜ)* vol. 99, 2019, pp. 81–99, [Online]. Available: https://doi.org/10.1016/j.cose.2022.102677

[115] D. Pal, X. Zhang, S. Siyal, "Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling

approach," *Technology in Society* vol. 66, no. 101683, 2021, [Online]. Available: https://doi.org/10.1016/j.techsoc.2021.101683

[116] A. Cirne, P. R. Sousa, J. S. Resende and L. Antunes, "IoT security certifications: Challenges and potential approaches," *Computers & Security,* vol. 116, no. 102669, 2022, [Online]. Available: https://doi.org/10.1016/j.cose.2022.102669

[117] J. Pirayesh, A. Giaretta, and M. C. P. Keshavarzi, "PLS-HECC-based device authentication and key agreement scheme for smart home networks," *Computer Networks*, no. 109077, 2022, [Online]. Available: https://doi.org/10.1016/j.comnet.2022.109077.

[118] M. Friedemann and C. Floerkemeier, "From the internet of computers to the Internet of Things," *From active data management to event-based systems and more*, Berlin Heidelberg: Springer, pp. 242-259, 2010. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-17226-7_15

[119] J. M. Batalla, A. Vasilakos and M. Gajewski, "Secure smart homes: opportunities and challenges," *ACM Comput. Surv*. vol. 50, no. 75, Sep. 2017, [Online]. Available: https://dl.acm.org/doi/10.1145/3122816

[120] J. S. Chavis, M. Doster, M. Feng et al, "A Voice Assistant for IoT Cybersecurity," *2021 IEEE Integrated STEM Education Conference (ISEC)*, 2021, pp. 165-172, [Online]. Available: https://ieeexplore.ieee.org/document/9764005

[121] P. Legg, T. Higgs, P. Spruhan, J. White and I. Johnson, "'Hacking an IoT Home'": New opportunities for cyber security education combining remote learning with cyber-physical systems," in *2021 Int. Conf. Cyber Situational Awareness, Data Anal. Ass. (CyberSA)*, 2021, pp. 1-4, [Online]. Available: https://ieeexplore.ieee.org/document/9478251

[122] L. Jixing, W. Yu and Q. Bin, "Discussion on Cyber Security Awareness and Awareness Model Building Based on Connectionism," in *2018 IEEE 4th Info. Tech. and Mechatronics Eng. Conf. (ITOEC)*, 2018, pp. 259-263, [Online]. Available: https://ieeexplore.ieee.org/document/8740446

[123] E. Schiller, A. Aidoo, J Fuhrer, J. Stahl, M. Ziörjen and B. Stiller, “Landscape of IoT security,” *Computer Science Review*, vol. 44, no. 100467, 2022, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013722000120

[124] F. Alghayadh and D. Debnath, "HID-SMART: hybrid intrusion detection model for smart home," *2020 10th Ann. Comp. Comm. Workshop Conf (CCWC)*, 2020, pp. 0384-0389, [Online]. Available: https://ieeexplore.ieee.org/document/9031177

[125] N. Elsayed, Z. S. Zaghloul, S. W. Azumah and C. Li, "Intrusion Detection System in Smart Home Network Using Bidirectional LSTM and Convolutional Neural Networks Hybrid Model," in *2021 IEEE International Midwest Symposium on Circuits and Systems* (*MWSCAS*), 2021, pp. 55-58, [Online]. Available: https://ieeexplore.ieee.org/document/9531683

[126] E. D. Alalade, "Intrusion detection system in smart home network using artificial immune system and extreme learning machine hybrid approach," in 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), 2020, pp. 1-2, [Online] Available: https://ieeexplore.ieee.org/document/9221151

[127] M. K. Kuyucu, Ş. Bahtiyar and G. İnce, "Security and Privacy in the Smart Home: A Survey of Issues and Mitigation Strategies," *2019 4th International Conference on Computer Science and Engineering (UBMK)*, 2019, pp. 113-118, [Online] Available: https://ieeexplore.ieee.org/document/8907037

[128] V. Williams, S. Terence J. and J. Immaculate, "Survey on Internet of Things based smart home," *2019 Int. Conf. Intelligent Sustainable Systems (ICISS)*, 2019, pp. 460-464, [Online]. Available: https://ieeexplore.ieee.org/document/8908112

[129] O. Lourme and M. Hauspie, "Toward a realistic intrusion detection system dedicated to smart-home environments," in *2021 17th Int. Conf. Wireless and Mob. Comp., Netw. Comms (WiMob)*, 2021, pp. 80-85, [Online]. Available: https://ieeexplore.ieee.org/document/9606337

[130] P. Nespoli, D. Díaz-López and F. G. Mármol, “Cyberprotection in IoT environments: A dynamic rule-based solution to defend smart devices,” *J. Info. Sec.*

Appl., vol. 60, no. 102878, 2021, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214212621001058

[131] D. Mocrii, Y. Chen and P. Musilek, “IoT-based smart homes: A review of system architecture, software, communications, privacy and security”, *IoT* no. 1–2, 2018, pp. 81–98, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S2542660518300477

[132] S. Bahizad, "Risks of increase in the IoT devices," in *2020 7th IEEE Int. Conf. Cyber Sec. Cloud Comp. (CSCloud)* 2020, pp. 178-181, [Online]. Available: https://ieeexplore.ieee.org/document/9170977

[133] “Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products”, NIST, Feb. 2022, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

[134] M. Fagan, J. Marron, K. G. Brady, Jr., B. B. Cuthill, K. N. Megas and R. Herold, “IoT device cybersecurity guidance for the federal government: IoT device cybersecurity requirement catalog”, NIST Special Publication, 800-213A, NIST, Nov. 2021, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf

[135] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS)”, NIST Special Publication 800-94, NIST, Feb. 2007, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

[136] M. M. Pillai and A. Helberg, "Improving Security in Smart Home Networks through user-defined device interaction rules," *2021 IEEE AFRICON*, 2021, pp. 1-6, [Online]. Available: https://ieeexplore.ieee.org/document/9570969

[137] C. M Ashworth, “Structured systems analysis and design method (SSADM), Information and Software Technology, Volume 30, 1988, pp. 153-163, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/0950584988900626

[138] K. Ito, S. Morisaki, A. Goto, “IoT Security-Quality-Metrics Method and Its Conformity with Emerging Guidelines”. IoT 2021, 2021, pp. 761-785. [Online]. Available: https://www.mdpi.com/2624-831X/2/4/38

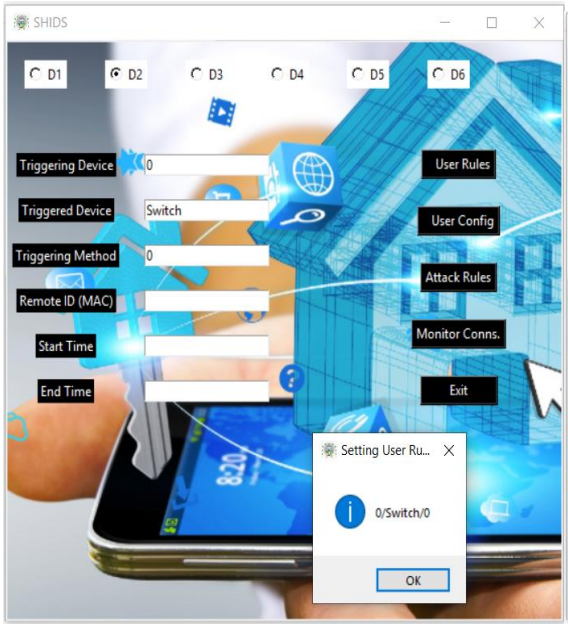
[139] M. T. Siponen, "Secure-system design methods: evolution and future directions," in IT Professional, vol. 8, no. 3, pp. 40-44, Jan.-Feb. 2006, doi: 10.1109/MITP.2006.73.

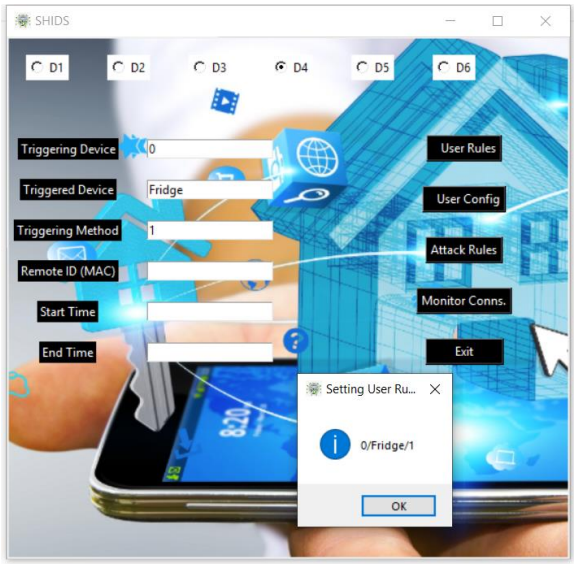
[140] S. H. Mirjalili and A. K. Lenstra, "Towards a Structural Secure Design Process," 2010 Fourth International Conference on Emerging Security Information, Systems and Technologies, Venice, Italy, 2010, pp. 280-286, doi: 10.1109/SECURWARE.2010.52.

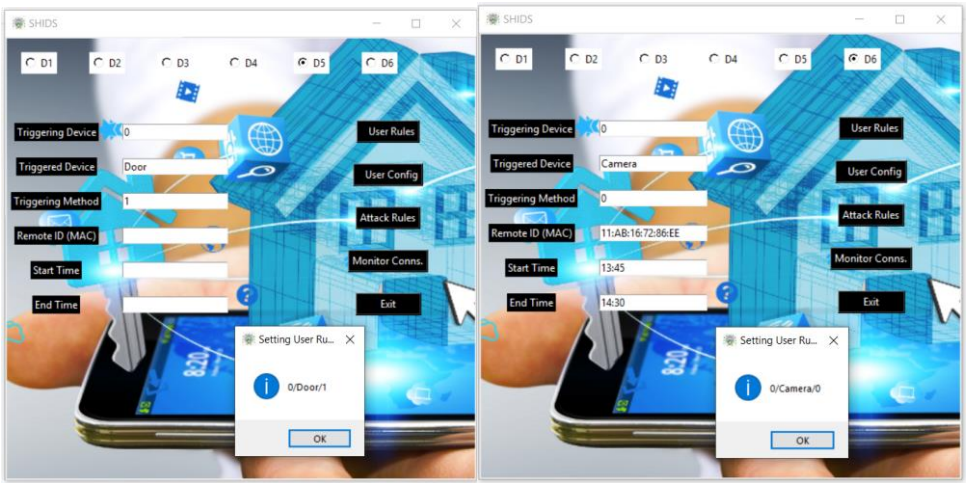
[141] N. Soudani, B. G. Raggad and B. Zouari, "A formal design of secure information systems by using a Formal Secure Data Flow Diagram (FSDFD)," 2009 Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS 2009), Toulouse, France, 2009, pp. 131-134, doi: 10.1109/CRISIS.2009.5411965.

Appendix A

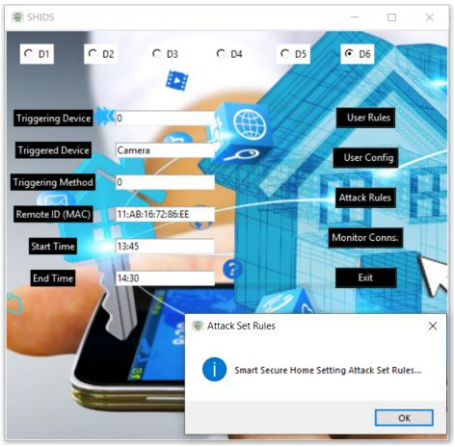
Appendix A consists of screenshots of the functionality in the prototype. The screenshot of each device configured in the prototype and how intrusions are triggered and detected is also displayed.





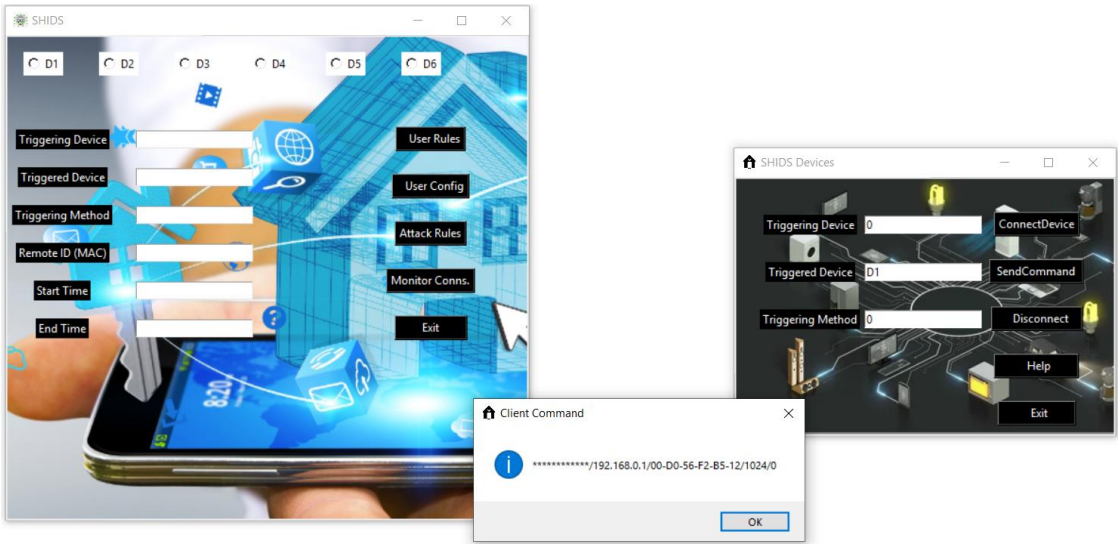


Appendix Figure 1: Set up of user configuration for all devices and rules formed

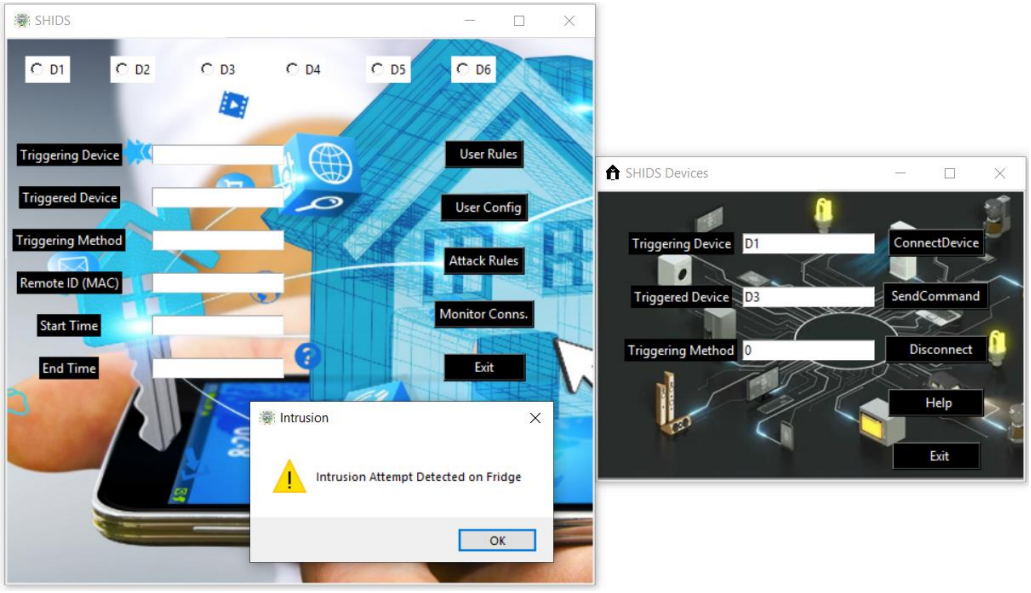


Appendix Figure 2: Setting up attack rules in a dataset using the IoT network dataset

Appendix Figure 3: Client (Smart Home Devices) connecting to the Smart Hub



Appendix Figure 4: Safe connections passed (same as user configuration)-intrusion not detected



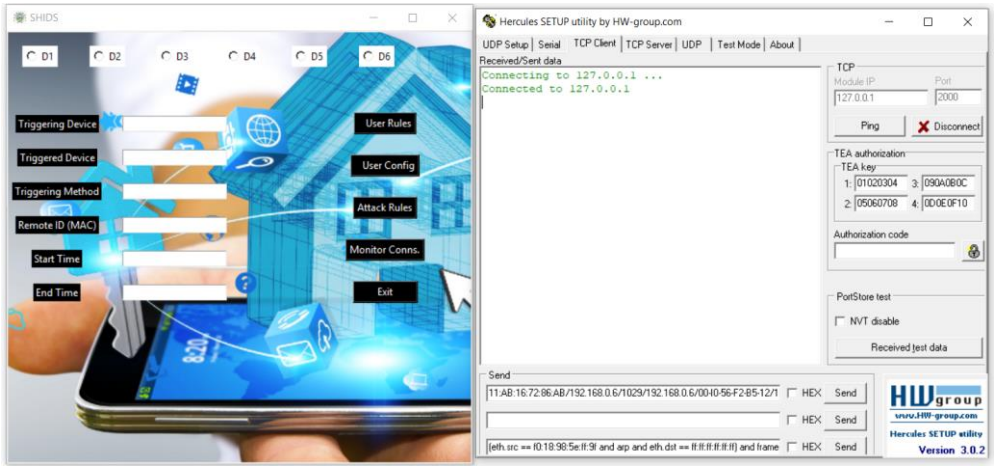
Appendix Figure 5: Intrusions passed to device 3-intrusion detected

USER_RULE_SET - Notepad

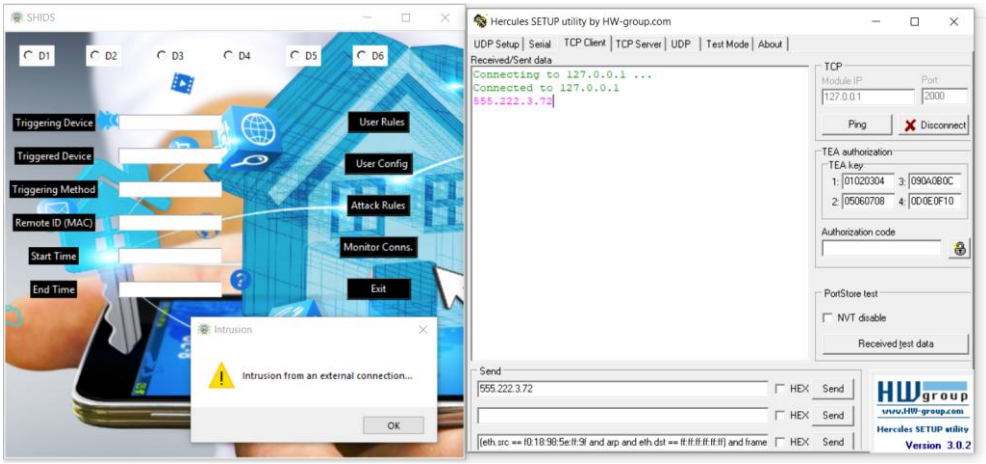
File Edit Format View Help

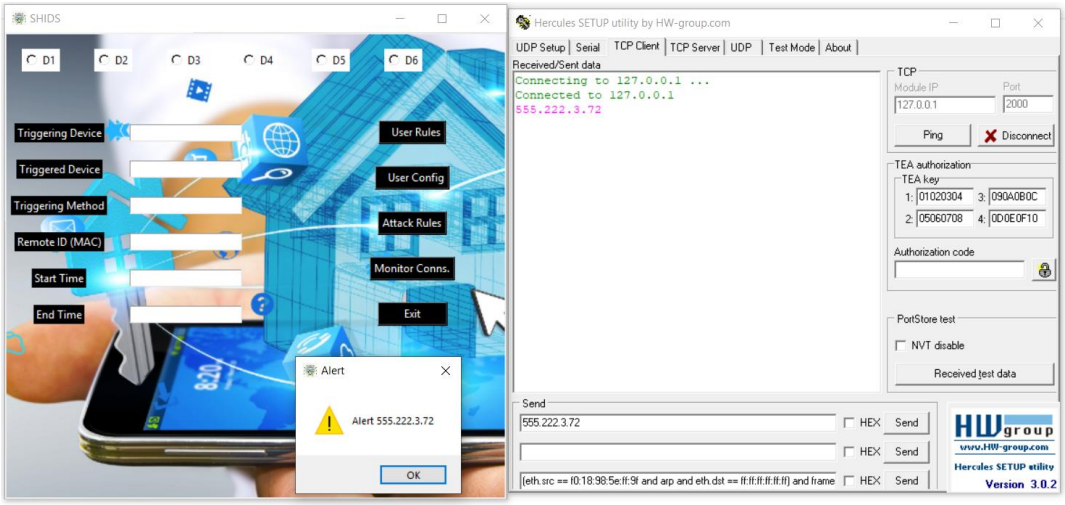
```
**********/192.345.23.1/DGH23456789123/2~2~
192.345.23.2/192.345.23.1/DGH23456789123/2~0~
192.345.23.3/192.345.23.1/DGH23456789123/2~0~
192.345.23.4/192.345.23.1/DGH23456789123/2~0~
192.345.23.5/192.345.23.1/DGH23456789123/2~0~
192.345.23.6/192.345.23.1/DGH23456789123/2~0~
**********/192.345.23.2/DGH23456789890/2~0~
192.345.23.1/192.345.23.2/DGH23456789890/2~1~
192.345.23.3/192.345.23.2/DGH23456789890/2~0~
192.345.23.4/192.345.23.2/DGH23456789890/2~0~
192.345.23.5/192.345.23.2/DGH23456789890/2~0~
192.345.23.6/192.345.23.2/DGH23456789890/2~0~
192.345.23.2/192.345.23.3/DGH23456789567/2~0~
192.345.23.4/192.345.23.3/DGH23456789567/2~0~
192.345.23.5/192.345.23.3/DGH23456789567/2~2~
192.345.23.6/192.345.23.3/DGH23456789567/2~0~
192.345.23.1/192.345.23.4/DGH23456789654/2~0~
192.345.23.2/192.345.23.4/DGH23456789654/2~0~
192.345.23.5/192.345.23.4/DGH23456789654/2~0~
192.345.23.6/192.345.23.4/DGH23456789654/2~0~
**********/192.345.23.5/DGH23456789233/2~0~
192.345.23.1/192.345.23.5/DGH23456789233/2~0~
192.345.23.2/192.345.23.5/DGH23456789233/2~0~
192.345.23.3/192.345.23.5/DGH23456789233/2~0~
192.345.23.4/192.345.23.5/DGH23456789233/2~0~
192.345.23.6/192.345.23.5/DGH23456789233/2~0~
**********/192.345.23.6/DGH23456789112/2~0~
192.345.23.1/192.345.23.6/DGH23456789112/2~0~
192.345.23.2/192.345.23.6/DGH23456789112/2~0~
192.345.23.3/192.345.23.6/DGH23456789112/2~0~
192.345.23.4/192.345.23.6/DGH23456789112/2~0~
192.345.23.5/192.345.23.6/DGH23456789112/2~0~
```

Appendix Figure 6: Data set of user rules that reflect all intrusions



Appendix Figure 7: Hercules connecting to the smart hub to connect to devices.





Appendix Figure 8: External connections present in IoT network data set sent to smart hub- Intrusions detected