Bachelor’s thesis

Information and Communications Technology

2022

Mayfred Appiah

IoT-based smart home: benefits, risks, solutions, and the AI developments for cyber defense

TURKU AMK

TURKU UNIVERSITY OF
APPLIED SCIENCES

Bachelor's Thesis| Abstract

Turku University of Applied Sciences

Information and Communications Technology

2022 | 46 pages

Mayfred Appiah

IoT-based smart home: benefits, security risks, solutions, and the AI developments for cyber defense

The ubiquity of the Internet of Things(IoT) has raised many privacy and security concerns for interconnecting networks and devices. Smart homes are a large part of IoT that presents itself in the everyday life of the human population. It is made of multiple devices in a home, controlled both locally and remotely, which aims to increase efficiency, comfortability and productivity via automation. Because of the smart home system's constant collection of data of the home environment, it also poses a security risk if targeted by malicious individuals. There are several traditional methods such as the Intrusion Detection System for defending against different types of attacks, however, by using Artificial Intelligence (AI), the security of the smart could be far more improved. The Artificial Intelligence methods explored in this thesis via the study of previous research and implementation by experts are Machine Learning (ML), Intelligent Agents, and Artificial Neural Networks (ANNs). Although traditional cyber security mesures work, they are not as efficient as the AI methods mentioned in this thesis. This thesis aims to answer the question of how AI can be used in improving cybersecurity in IoT-based smart homes. After reading this thesis, one would be familiar with the architecture and security of an IoT-based smart home and the developments made in protecting them from threats, traditionally and with Artificial Intelligence.

Keywords:

Internet of Things, Smart homes, Machine learning, Cyber security, Artificial Inteligence

Opinnäytetyö (AMK) | tiivistelmä

Turun ammattikorkeakoulu

Tieto-ja vietsintätekniikka

2022 | 46 sivua

Mayfred Appiah

IoT-pohjaiset älykodit, hyödyt, turvallisuusriskit, ratkaisut ja tekoälyn kehitys kyberpuolustukseen

Internet of Things (IoT:n) teknologian yleisyys on herättänyt monia tietosuoja- ja turvallisuusongelmia kysymyksiä verkkojen ja laitteiden yhteen liittämisessä. Älykodit ovat iso osa IoT:tä, joka on ihmisten jokapäiväisessä elämässä. Se on koostunut useista kodin laitteista, joita ohjataan sekä paikallisesti että etänä. Älykotien tavoitteena on lisätä tehokkuutta, mukavuutta ja tuottavuutta automaation avulla. Älykodin järjestelmä kerää jatkuvasti kotiympäristön dataa. Tämä aiheuttaa myös turvallisuusriskin, jos älykoti joutuu ilkivalan kohteeksi. On olemassa useita perinteisiä tapoja, kuten tunkeilijan havaitsemisjärjestelmä, jolla suojaudutaan erilaisia hyökkäyksiä vastaan. Käyttämällä tekoälyä älykodin turvallisuutta voitaisiin parantaa paljon enemmän. Tämän opinnäytetyön tavoitteena oli vastata kysymykseen, kuinka tekoälyä voidaan käyttää kyberturvallisuuden parantamiseen IoT-pohjaisissa älykodeissa.Tässä opinnäytetyössä tutkittuja tekoälymenetelmiä ovat koneoppiminen (ML), älykkäät agentit ja Artificial Neural Networks (ANN). Perinteiset kyberturvallisuusmenetelmät toimivat, mutta ne eivät ole yhtä tehokkaita kuin opinnäytetyössä mainitut tekoälymenetelmät, jolla parannetaan turvallisuutta.

Asiasanat:

Internet of Things, älykodit, koneoppiminen, kyberturvallisuus, tekoäly

Content

List of abbreviations (or) symbols 6

1 Introduction 8

2 IoT-based smart homes 11

2.1 Types of smart homes and users 13

2.2 Internet of Things 14

2.2.1 IoT architecture 15

2.3 Benefits of smart homes for its residents 20

3 The security risks of IoT-based smart homes 22

3.1 IoT Cybersecurity and threats on the devices 25

3.1.1 Attack types on the Application layer 27

3.1.2 Attack types on the Perception layer 28

3.1.3 Attack types on the Network layer 29

3.1.4 Attack types on the Physical layer 31

4 Improving cybersecurity with AI 33

4.1 Machine Learning: supervised, unsupervised and reinforced learning 34

4.2 Intelligent agents 35

4.3 Artificial neural networks 36

4.4 Computer vision 38

5 Conclusion 41

References 43

Figures

Figure 1. Prediction of IoT growth [10]. 14

Figure 2. Action taken from the sensor to an actuator [14]. 17
Figure 3. Three Layer IoT Architecture [15]. 17
Figure 4. Four-layer architecture [16]. 18
Figure 5. Five Layer IoT Architecture [17]. 19
Figure 6. A smart sensor alerting of a fall [8]. 21
Figure 7. The PROs and CONs of IoT [6]. 22
Figure 8. Cybersecurity threat landscape [8]. 26
Figure 9. A man-in-the-middle attack between a client and a server [1]. 30
Figure 10. An Intelligent Agent Cyber Police at the beginning of a cyber-attack [27]. 36
Figure 11. ANN preventing an attack in an ISA [27]. 37

List of abbreviations (or) symbols

Abbreviation	Explanation of abbreviation (Source)
AI	Artificial Intelligence
AES	Advanced Encryption Standard
ANNs	Artificial Neural Networks
ARP	Address Resolution Protocol
DDos	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
ICT	Information and Communications Technology
IDS	Intrusion Prevention Service
IDPS	Intrusion Detection Prevention System
IoT	Internet of Things
IPS	Intrusion Prevention System
IP address	Internet Protocol Address
ISA	Integrated Security Approach
k-NN	K-Nearest Neigbours
ML	Machine Learning
MITM attack	Man In The Middle Attack
MQTT	Message Queuing Telemetry Transpot
NB	Näive Bayes
NFC	Near Field Communication
PDoS	Permanent Denial of Service

RFID	Radio Frequency Identification
RSA	Rivest-Shamir-Adleman
SSL certificate	Secure Sockets Layer certificate
SHAP	SHAPley Additive exPlanations
RFID	Radio Frequency Identification
WSN	Wireless Sensor Networks
SSL certificate	Secure Sockets Layer certificate

1 Introduction

The increased usage of the Internet of Things (IoT) has been efficient and could be described as a blessing to the world in terms of connectivity as it has given the population, “accessibility, integrity, availability, scalability, confidentiality, and interoperability” [1] in daily activities. However, there have been many concerns regarding its security due to its high connectivity and interwoven networks on which it operates.

Internet of Things (IoT) refers to physical devices connected to the internet, each other, and users. Smart homes are a part of the Internet of Things. The IoT aspect is what provides devices access to the internet as well as the interconnectivity that enables devices to connect with each other. From a technical point of view, a smart home is defined with the objective to control smart devices remotely using the internet in a home environment. It also allows for the automation of the control of the devices such as lighting system, ventilation, and air conditioning system. Since context-awareness is a crucial factor of IoT, automation calibrates the devices to monitor, have access to, and control the environment, using its various sensors and network. [2,3]

A smart home can be described as a home that is automated using the IoT model and is adaptive and reactive to conditions and demands of the environment and users [3]. Today, the popularity of smart homes is high among all demographies but particularly high in recent times amongst elderly and physically challenged homes. The elderly generation is an ever-increasing group that is projected to increase even more. In the United States, for example, the number of older adults is expected to reach 21% from the current 16% by the year 2040 [4]. Europe is often referred to as the ageing continent due to low birth and increase in the older population. Many research studies are thus being conducted at the societal level on the risks and benefits of IoT and smart homes; how they can be used to minimize how the younger population are affected by the population grwoth of the elderly and how to aid older adults, the elderly, and the disabled in living independently and comfortably.

This will also help financially as being supervised by smart home systems is thought to be more cost-effective than having a nurse.

However, due to the interconnectivity and complexity of smart home devices, there exist numerous security risks, that is, the heterogeneity of IoT makes them extremely vulnerable. Several traditional security methods, such as the Intrusion detection system (IDS), are not as effective in tackling IoT security issues due to the rapid growth of data. Thus, many scholars or modern security approaches have been advancing the need to incorporate AI in tackling the security threats IoTs face. Fortunately, one of the main applications of AI in the daily lives of the populace is IoT and smart home devices, so this line of argument has had warm responses.

Artificial Intelligence is more than Machine Learning (ML), there are many branches and related fields such as Expert Systems and Fuzzy Logic, however, this thesis focuses on how Machine learning, Intelligent agents, and Artificial Neural Networks (ANN) are used in improving cybersecurity. ML is used in the application and automation of IoT smart homes, and it has proven useful in their protection from cybersecurity attacks. Although AI and Machine Learning have been used to thwart cyber-attacks and their development, a great advantage for cybersecurity is cyber defence. This solution is , however, penetrable as hackers have also developed sophisticated ways including the use of Artificial Intelligence for attacks. Thus as the usage of IoT grows, so do security concerns.

Since IoT, smart homes, cybersecurity, and AI are all broad concepts that cannot be exhausted in this thesis, the focus is on the intersection between AI, cybersecurity, and smart homes. In short, AI for improving cybersecurity in smart homes type of IoTs. The main question that this thesis aims to answer is how AI can be used in improving the cybersecurity of smart-home-based IoTs.

Chapter 1 introduces the topic and sets out the parameters within which the key concepts, issues, and approaches will be looked at in this paper. Chapter 2 focuses on smarts homes, what they are, their importance, the key features of smart homes, devices, types of smart homes, smart-homeowners before focusing on IoT-based smart homes; what they are, features that make them different from other smart homes, and how relevant this type of smart homes is to their users. Chapter 3 discusses the security risks, challenges, and threats of smart homes in general and IoT-based homes with an emphasis on the current solutions for IoT-based smart homes. Chapter 4 builds on its preceding chapter to analyze the varied ways AI can be used to protect IoT-based smart homes and/or enhance existing solutions or security systems in place. The studies on AI in IoT and other areas where AI have been used in cyber defence are a feature used to buttress this point with cogent examples. The concluding Chapter 5 summarizes the findings in this paper with additional suggestions.

In addition, figures diagrams and pictures are employed in illustrating some of the concepts and mechanisms. This is an explanatory thesis.

2 IoT-based smart homes

In this chapter, the setup, structure, and architecture behind IoT based smart homes are examined, as well as the various elements that make a smart home sync up as one unit. The smart home system is also disintegrated to expose the possible weaknesses for a deeper understanding of how IoT-based smart homes operate.

Smart homes are broadly defined under two wide categories, the first group focuses on a smart home as a home and what it can do for its users. Darby [5] defined a smart home as a “residence equipped with communications networks, linking sensors, domestic appliances, and devices, that can be remotely monitored, accessed, or controlled and which provides services that respond to the needs of its inhabitants”. In general, they consist of smart objects. Smart objects are devices or objects that learn from users’ behaviour, and their surroundings to decide the action to be taken based on a data set. [5]

Smart devices possess some level of machine intelligence. A device is, therefore, not considered smart if it acts solely on a user’s instruction to perform a task. Likewise, the mere collection and transfer of data do not make a device smart, rather, if the machine utilizes the data and can predict and makes decisions by itself based on the data it collected, it could then be defined as a smart device. [6] Examples of smart devices that fall under this definition include fridges, television, washing machines, and environmental systems such as HVAC (Heating, Ventilation, and Air-condition) and light control [4]. Silverio-Fernández, Renukappa, and Suresh 2018 in their study [2] believe that smart devices are designed to interact with users and other devices. A device that does not interact with other devices is not a smart device based on the aforementioned article however, user interaction is not essential for a device to be considered smart.

The second set of definitions, however, is more building and system-focused, “Smart buildings are flexibly connected and interacting with the energy system, being able to produce, store and/or consume energy efficiently.” [5]

Based on the two categories of definitions, a smart home can be considered as an IoT solution in a home environment that allows monitoring of its residents with the aim of improving their living conditions [7]. They are multiple devices connected to each other in a home, made to increase efficiency (in energy consumption and electricity), productivity, automation, safety, security, and comfortability [6]. The devices can be managed via a WIFI connection or a central monitoring system such as Google Nest Hub [8].

Smart home automation can be divided into two types: “locally controlled or remotely controlled systems.” That is, smart devices and systems can either be controlled locally through ‘hubitat’ which is a smart home hub, or a cloud independent hub that works as the central control system or remotely. Remotely controlled systems, on the other hand, utilize the internet and cloud to allow users to control their smart home with a cloud-controlled hub, mobile device, tablet, or computer, whereas locally controlled system uses private smart automation hubs to control the automation process. [3]

An example of a remotely controlled system would be a resident forgetting to turn the stove off while going out, in this case, using an IoT-based smart home system, they would be able to turn the stove off remotely from wherever they are at. The central monitoring system allows for remote control of the devices connected to it, which also increases the chance of the system being compromised. A smart home is built on a hub that allows users interaction and control of the smart home, for example, Amazon Echo and Google Home [8].

IoT-based smart systems are able to provide remote access and reactive analysis of the environmental changes when the IoTs are applied using dynamic database management [7]. To resolve challenges raised by realistic application, Ghayvat et al. [7] implemented a smart home based on an integrated framework that used the past, real-time, and feedback data for its analysis. The reason for this was to resolve issues that may raise false attempts by separating the normal routine data from unexpected data. [7]

2.1 Types of smart homes and users

There are various kinds of smart homes for different services, such as ones catered to entertainment, energy efficiency, or residential spaces like the elderly, healthcare, and childcare-centred living spaces. Toyota dream house in Japan, e-House by Mcdonough in New York, and Crystal House by Hung in Taiwan are industrial smart building/home services that focus on sustainability, energy efficiency, and comfortability through using the Intelligent environment [7].

There are also smart homes designed and developed to look over elderly people living alone. These types of smart homes can monitor the physical, physiological, and environmental changes. As a result of smart home sensors being used to monitor the elderly, some studies have shown that the employment of nurses might be hit negatively as they might not be needed as much in elderly care homes and in-home care as smart home solutions continue to develop. [6]. However, due to the ageing population, this might not become an issue as instead of replacing homecare nurses, smart homes will subsidize this area whilst nurses are given more urgent tasks because of the rise in demand for the healthcare workforce. An older person who does not live with their families is prone to feel lonely and want to have human company often. The IoT solution of checking their health remotely and having no nurse is a cause of concern in that aspect.

There are several types of smart home users. In the paper by Mare et al. [9], the point of view of three different smart home users is studied. The users are the primary user, the secondary user, and the guest user. Based on the type of user, the resident will have a different access control level. Different smart homes support different amounts and types of users. Apple home has two different users, the primary and secondary users. The primary user has owner privileges whereas the secondary user can control the devices but cannot add or remove users and devices. In Apple home, the primary user can tweak the privileges of the secondary user to give them more access control. It also supports guest mode which places restrictions such as not being able to remotely control the home from outside the house. On the other hand, Google Home and Amazon Echo do not support multiple users.[9]

2.2 Internet of Things

A smart home is part of the Internet of Things (IoT), however not all IoT are smart homes. IoT is a technology in which physical devices connect to the internet and each other to collect, generate and provide information. When looked at from the perspective of a smart home, IoT can be defined as connecting household devices, electrical appliances, sensors, and actuators to the Internet, it is the component of the smart home that enables smart devices to be remotely controlled. The rise of IoT is expected to continue and it has been predicted that by the year 2040, the number of IoT devices will be about 140 billion as shown in Figure 1 below [10].

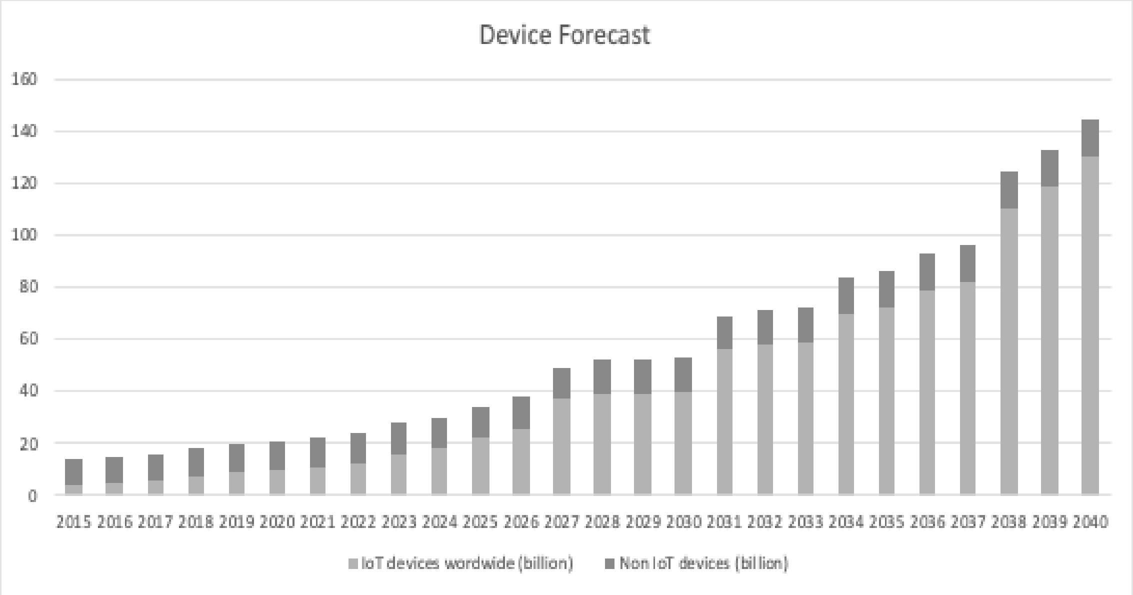


Figure 1. Prediction of IoT growth [10].

IoT devices encourage digitalization and improve efficiency by gathering data and applying machine learning algorithms. Context awareness, connectivity, and autonomy are key factors of IoT and smart devices, they should be able to communicate with other devices and operate based on those data autonomously [2]. Connectivity in IoT means establishing a connection between the devices, intranet, or the internet. Connection to the internet is extremely common in smart devices. Context-awareness is the ability and capability of a device to perceive information/data collected from the sensors. The device is then able to make autonomous decisions based on the data and help the user.

Since data collected by IoT grows exponentially each day, Big Data makes it easier to handle such a massive and growing amount of data [6]. Big Data is a massive amount of structured, semi-structured, and unstructured data that comes in huge continuous volumes and speed and thus cannot be processed in the traditional way, for example, Facebook data. 500+ terabytes of data are generated on Facebook daily [6]. Big Data and IoT highly rely on each other as smart home devices are continuously gathering and processing huge amounts of data. It optimizes the analysis of the data collected by IoT [11]. IoT utilizes cloud storage as smart devices do not have unlimited data storage capabilities for the amount of data generated.

2.2.1 IoT architecture

The core infrastructure of an IoT framework/technology consists of these independent units: sensors, actuators, servers, and communication networks that operate in unison to provide a smart experience.

The communication network is what an IoT uses to communicate with neighbouring devices and to the internet. Some of the communication methods protocols used in IoT are WIFI, NFC, Bluetooth, MQTT (Message Queuing Telemetry Transport and Zigbee.

Servers are a machine or computers that process the requests made by a user, for example, when a user makes a google search, the server receives the request, processes it and then sends the response or results to the user. There are some different types of servers for specific tasks such as mail server, application server, and cloud server which are very relevant to the IoT system.

A sensor is a very important part of smart objects. All IoT applications must have one or more sensors to gather data from the environment. Context awareness, which is one of the most important characteristics of IoT would not be possible without sensors [12]. Sensors are more common in everyday life than one would think, for example, motion sensors are used when an escalator starts moving when you get on and a supermarket door opens for you. Other sensors would include a camera, temperature sensors in a thermostat, and smoke sensors in a smoke alarm. Machine learning algorithms may also be applied to the data collected by sensors such as through smartphones in order to get accurate data, that is recording running instead of walking when one is running.

An actuator is a device that can change electrical energy into another type of useful energy. The different kind of actuators in IoT are; hydraulic actuators, which converts hydraulic energy into useful work; pneumatic actuator, which converts electrical energy into mechanical motion; thermal actuator, which produces motion due to temperature changes; electrical actuator, which converts electricity to kinetic energy; magnetic actuator which “converts an electric current into a mechanical output and relay actuators of which the majority uses “electromagnets to mechanically operate a switch [13]. Figure 2 is an image of how information collected by the sensor is sent to the control centre which dictates an action that is taken by the actuator, in this case, the sprinkler turning on.

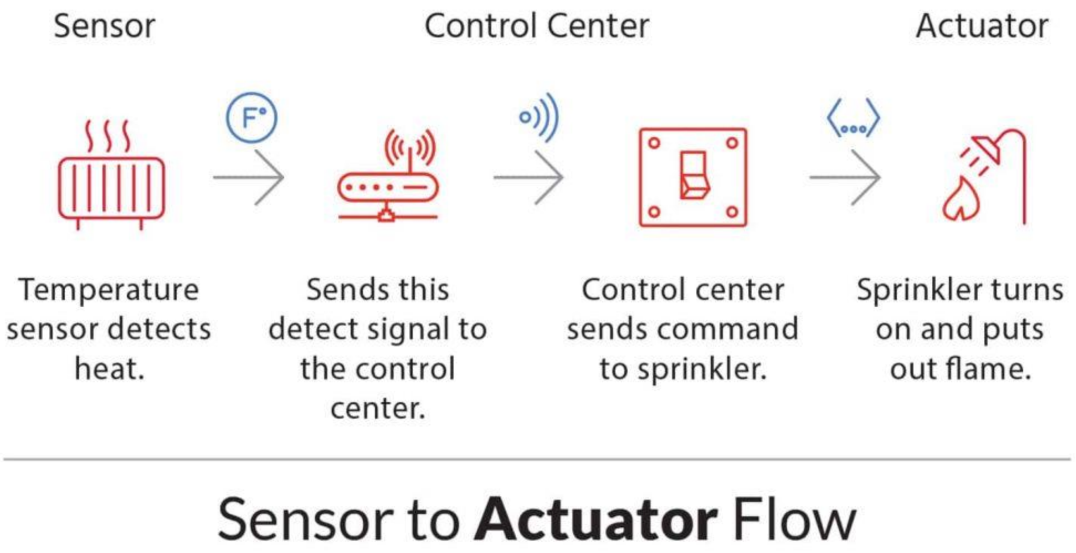

Sensor
Control Center
Actuator
F°
Temperature sensor detects heat.
Sends this detect signal to the control center.
Control center sends command to sprinkler.
Sprinkler turns on and puts out flame.
Sensor to Actuator Flow

Figure 2. Action taken from the sensor to an actuator [14].

Although there is not one standard IoT architecture, the most basic and widely accepted type is a three-layer and four-layer architecture(Figure 3). There is also a five-layer format and others which are also used when needed to focus on details of IoT. These are all called protocol architecture. [12]

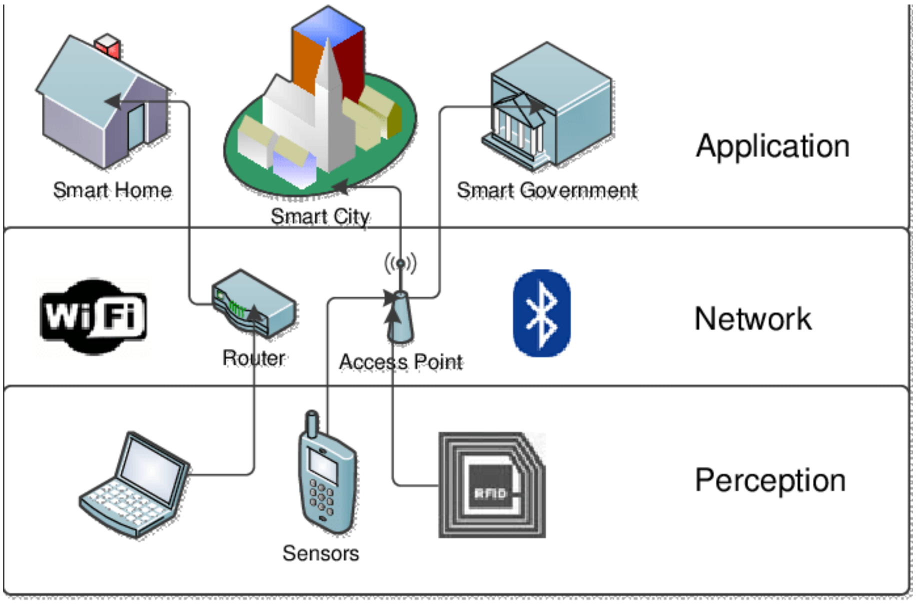


Figure 3. Three Layer IoT Architecture [15].

The three-layer architecture includes the perception layer, the network layer, and the application layer. Figure 3 and Figure 4 examples of the layers of the three-layer and four-layer architecture respectively, and what they entail. The perception layer is also the physical layer in this architecture. It gathers data using its sensors and connected devices. It also senses and recognizes other smart objects in the environment. The network layer's responsibility is to process and transmit all the data collected by the perception layer. Its job also includes connecting to other smart objects, servers, and network devices. The application layer connects the network and IoT devices, it delivers application services to the user, such as a user clapping their hands to turn lights off. [12]

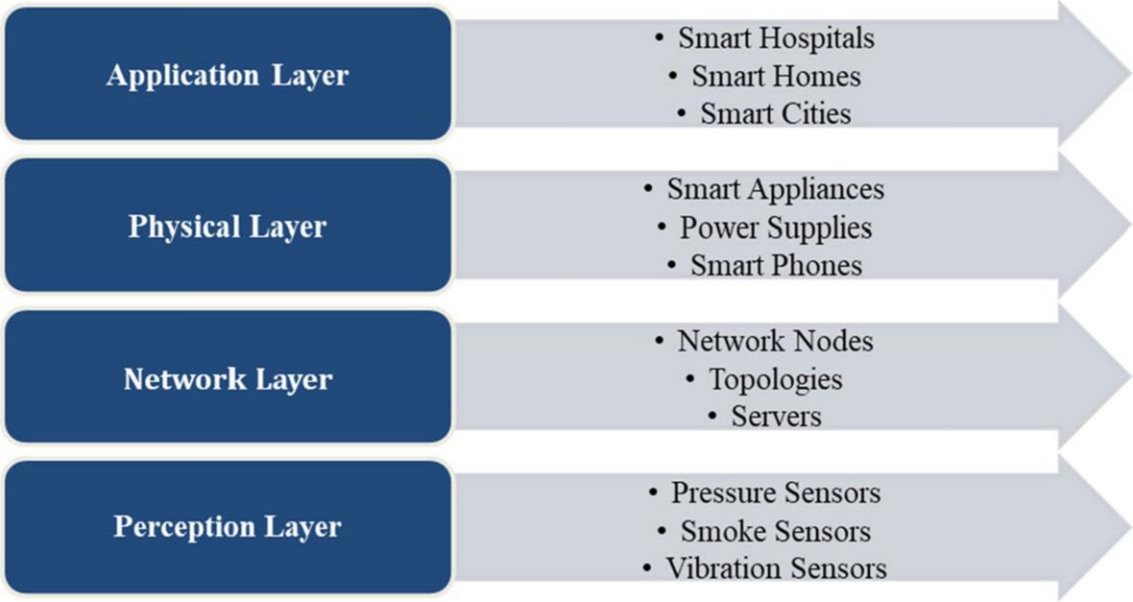


Figure 4. Four-layer architecture [16].

The five-layer architecture goes more in-depth. It adds three new layers to the perception and application layer. These new layers are the transport, business, and processing layer. The transport layer transfers the data collected by the sensors in the perception layer to the processing layer through the networks. The processing layer stores, analyses, and processes the huge amount of data received from the transport layer. It takes on many technologies, such as databases and cloud computing. The applications, business model, and user privacy are managed by the business layer. Figure 5 is the topology of a five-layer architecture. [12]

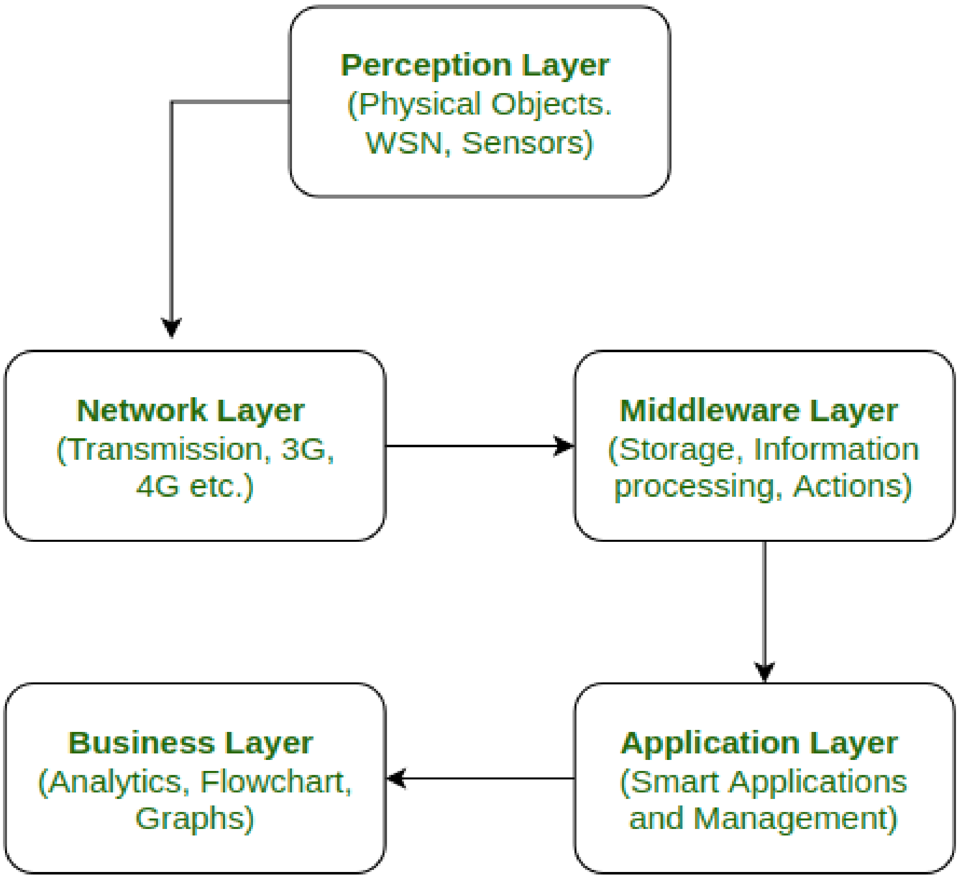

Perception Layer
(Physical Objects. WSN, Sensors)
Network Layer
(Transmission, 3G, 4G etc.)
Middleware Layer
(Storage, Information processing, Actions)
Business Layer
(Analytics, Flowchart, Graphs)
Application Layer
(Smart Applications and Management)

Figure 5. Five Layer IoT Architecture [17].

IoT devices connecting to the internet through Internet Protocol (IP) stack require a huge amount of power and memory from the connecting devices, however, devices can also be connected through non-IP networks. Non-IP networks do not consume as much power and connections happen locally. These non-IP network options such as Bluetooth, Radio Frequency Identification (RFID) and Near Field Communication (NFC) have limited range and power therefore, they cannot be used in large areas that require monitoring by multiple sensors. RFID and Wireless Sensor Networks (WSN) are important technologies used in IoT. “RFID is an identification technology”. An RFID reader reads data from an RFID tag (a chip with an antenna). The tag carries and stores the data, which is then transmitted using radio waves. WSN is made up of tens of thousands of sensor nodes connected using wireless technology. Data collected by the WSN is sent to the gateway device which then forwards the data to the cloud over the internet. [12,18]

2.3 Benefits of smart homes for its residents

As smart homes are designed to automate and facilitate everyday life to make living more comfortable and efficient, their increasing popularity cuts across all groups of people, while the young generation was born into the ICT (Information and Communication Technology) culture the matured group have found the incorporation of many smart home devices lifesaving with the elderly are virtual dependant.

Several studies have shown that smart homes are a great solution for those who are unable to manually do everyday activities due to disability or ageing. It allows them to be able to control and use different home appliances and make everyday life easy to navigate through [4]. However, it can also be used to help those who otherwise would need daily assistance from a nurse or a family member to cope daily such as the elderly or the disabled.

The continued ageing of the population, also known as the ageing of Europe, that is caused by low birth rate and increasing life expectancy; brings about issues, such as labour force shortages. Many solutions are being brought up to tackle the problems and a smart home solution is one of them. Many elderly people may have families to take care of them hence, some may not have family nearby or may not want to burden their family hence are living alone [6]. Home cares are a good solution, however not everyone can afford to do so, and this is where a smart home comes into the picture.

The solutions for the elderly and disabled do not differ much from the solutions for other groups of people, however, the way they are implemented is more well thought out and considered. There are healthcare devices that can be part of a smart home. Wearable sensors, such as an apple watch, help collect health data, such as heartbeat, blood pressure, and body temperature. Other sensors such as motion sensors, temperature sensors, and pressure sensors are also helpful in monitoring the health of an individual. [6]

Voice-controlled assistants, such as Google Assistant and Amazon Echo, are used in controlling a smart home with one's voice. This feature/technology is very useful for people with weak eyesight or the visually impaired. The elderly are prone to falling incidents which may be very harmful to them. This is where cameras sensors come into play, using its computer vision technique, a smart camera can detect a person falling and then send for help. Some smart homes utilize AI in addition to sensor data to help capture and analyze facial expressions, this can help in detecting the kind of emotional state the resident may be in or even detect an illness. [8]

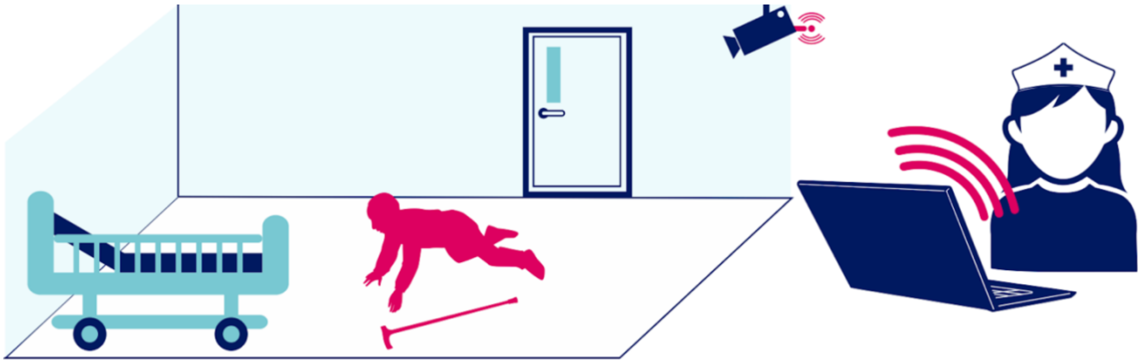


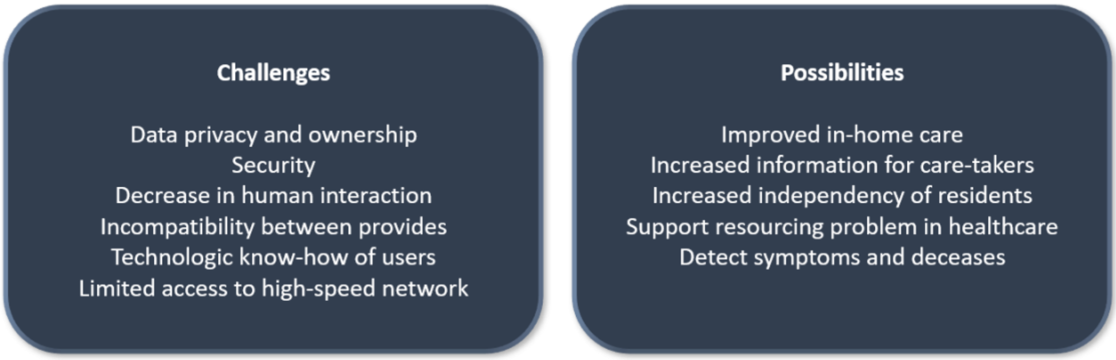
Figure 6. A smart sensor alerting of a fall [8].

If a resident has a caretaker who cannot be around 24/7, smart homes assist in providing the caretaker with information and alerting them in case of any incident as shown in the Figure 6.

3 The security risks of IoT-based smart homes

In this chapter, the security risks associated with having an IoT-based smart home are looked at, where they occur with the set-up/system, how they occur, as well as the common attacks that have been plaguing each layer of the IoT-based smart homes.

IoT faces numerous security and privacy challenges because of its complexity, heterogeneity, and connection between devices and the internet. As IoT usage increases, so will new issues and challenges in protecting their security and privacy arise. The following figure shows some of the challenges but also benefits of IoT-based smart homes, specifically for the elderly [6]. The security risks and worries of the increasing usage of IoT are often privacy-related however, other security risks such as malware compromising the device and controlling it and the “AI training data containing errors leading an accident” cannot be discounted [8].



Challenges

Data privacy and ownership
Security
Decrease in human interaction
Incompatibility between provides
Technologic know-how of users
Limited access to high-speed network

Possibilities

Improved in-home care
Increased information for care-takers
Increased independency of residents
Support resourcing problem in healthcare
Detect symptoms and deceases

Figure 7. The PROs and CONs of IoT [6].

The more complex a system is, the more it is susceptible to vulnerabilities, yet, IoT devices usually have a limited amount of data they can store; hence the need for a cloud for data storage and cloud computing. Many manufacturers, however, do not consider the classification of the data being in transmission when designing IoTs, this leaves data transmission vulnerable. Implementing encryption methods during this stage could help avoid some vulnerabilities. [19]

Smart home security is not up to par compared to a normal computer as they do not have high computer processing power, large storage space, or large memory size and are also limited in energy consumption [20]. Therefore, implementing traditional and intense security solutions such as Advanced Encryption Standard (AES) and RSA may not always be a viable option thus compromise has to be often made [3,20].

A consumer’s personal information, such as credit card information, home address, and phone number, is at risk with IoT devices since the devices are usually connected to one Wi-Fi network, as such if one device is breached, the others can also be easily accessed [6]. This makes it difficult to find the breached device.

Sensitive data gathered from a consumer might show the behaviour patterns of the user. Most of the time, consumers are not aware of how the data is used or how widely data can be accessed. The data being used in consumer analytics or medical research raises questions about the ethics of third parties' accessibility to the data [6]. For example, if an attacker notices an elderly resident in a family household is always home at a certain time, they might choose to send them a message pretending to be their grandchild needing money urgently. Using security strategies such as device management, access control, and encryption minimize vulnerabilities [21].

Many people, specifically older adults, are not aware of all the dangers in terms of security, threats and attack might unknowingly do something that puts a device at risk of being attacked. Several social engineering attacks are led against them as they are usually the most vulnerable. In social engineering, the attackers try to trick victims into giving them sensitive information such as social security numbers or credit card numbers. Human-based social engineering is done face-to-face and the one done via computer is termed a cyber-attack [16].

By raising awareness of the risks and vulnerabilities of IoT devices and how to use them without causing a security issue, the above issues can be tackled. In the research survey done by Zeng et al. [22], some participants connected their smart appliances to a different WIFI from other appliances in the home. Two participants took to block a certain type of traffic from their smart devices. One participant blocked all unencrypted traffic and the other blocked their hub from communicating with cloud servers, this user instead used a Message Queuing Telemetry Transport (MQTT) broker, a message protocol for messaging between IoT devices, to control it from a local server [22]. By using an MQTT broker, the user switched to a locally controlled smart home which is more secure than a remotely controlled one as the instructions do not go over through the internet. Deduced from this research, it seems that most users are privy to privacy concerns and have unconventional and technical ways to go about increasing their security, for example, it is only to turn google assistant or Alexa off while having a confidential conversation or old deleting camera recordings to increase privacy while others are unaware of the concerns.

The way the smart home hubs handle the data shared between the devices and users is extremely important to the security and privacy of the users. For example, with Apple and Google Home, the user owns the data and can delete the data, however with other smart homes such as Philips Hue and Wink, it is unclear who owns the data. There are three types of data shared between users in the evaluation done in the research by Mare et al. [9]. They are the user's location, automation, and device activity log. The data shared differs depending on the smart home, in Apple Home, the automation is shared and in Wink, only the device activity log is shared [9].

There are security risks to the device log activity being shared between users, firstly it allows other users access to the data and activity of various users in which case, a user might feel like they are being watched which would make them uncomfortable and a user with ill intent to cause harm to another may be able to spy on another based on their behavioural activity and succeed in their aim. Allowing guests to have certain access to one's smart home could pose a security threat when the guest leaves the premises but still have access to the home hence setting up location-based access would be useful in this situation as the guest loses access as soon as they are not present in the home. [9]

Smart home automation could be used to tackle an intruder by monitoring the activity pattern of the resident of a household. Scheduling the lights and appliances to turn on at certain times to throw a burglar off the fact that there is no person in the house is an example use of smart home automation. This area application is called energy control. Although it is not energy efficient, it increases the security and privacy of the smart home as it may deter intruders. [23]

The European Union (EU) has got legislations set to protect users' data, for example, a subject can have accessibility to view their data and ask for it to be deleted or sent to them. Also, raising awareness about the safe usage of IoT devices and teaching consumers about the risks and how to lessen them improves the device's safety and consumer privacy [6].

3.1 IoT Cybersecurity and threats on the devices

Cyber security faces several challenges as vulnerabilities are exploited in numerous complex and advanced ways. A problem with smart devices is that the security features do not compare to computers. IoT is gaining more traction and with the amount of data stored online and around 5 billion people connected to the internet, new difficulties and challenges continue to show up for which mitigating them through conventional ways will not always be viable [24].

This rise in usage of IoT appliances has caused challenges for cyber security due to insufficient encryption and poor mechanism for authentication of the ever-growing data. According to the paper, the role of Artificial Intelligence[25] in cybersecurity, 70% of IoT devices are vulnerable to security breaches and attacks [25].

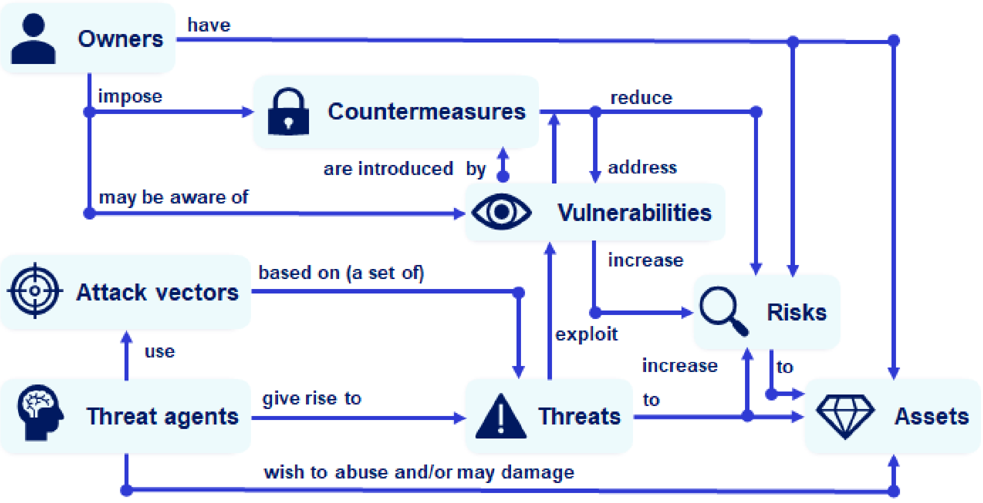


Figure 8. Cybersecurity threat landscape [8].

Threat agents use attack vectors to create a threat by exploiting a vulnerability in a network or system which can lead to the breach of a device[8]. Vulnerabilities are mistakes or errors, that leave a gap or make it easy for a threat to happen. Examples of vulnerabilities are system maintenance, using personal devices at work, password usage, etc.

A smart home can also have its own private network or intranet which is safer than being connected to the internet. The remote access of devices makes them more vulnerable to being accessed by an unauthorized person. When talking about the security of smart homes, the terms smart device or IoT device/appliances might be used often as these devices interconnected are what makes a smart home and an attack on one affects the other devices in the system.

Some of the security breaches might be caused by the gateway being compromised, they might also be caused by a compromised sensor node, a device being tampered with physically or by a natural occurrence such as an earthquake damaging the device [16]. The gateway is the doorway between the IoT devices and control devices (phones and tablets).

Successful attacks have happened over the years, for example, in 2014, more than 73000 video camera footage was found to be live streaming on the internet. In the same report, smart home security based on the four-layer architecture and their mitigation strategies is covered. [16]

There are different kinds of attacks that a smart home can be attacked with depending on the attacker’s objective and to protect the devices from attacks such as the one mentioned above, there are different strategies placed to fight threats and attacks. There are different IoT architectures such as three-layer, four-layer, and five-layer architecture as there is no standardized one, as such there are multiple attack surfaces. In the research by Touqueer et al.[16], the four-layer architecture was used, and the authors propose a framework that helps people to avoid attacks as well as present challenges such as device misconfigurations and malicious attacks. Each layer has its vulnerability therefore, having security at each layer strengthens the security of the smart home.

3.1.1 Attack types on the Application layer

In a phishing attack, the attackers usually get into the network by pretending to be someone close to the victim or using a fake website that is identical to an original one [16]. In doing this, the victims are confused and are led to believe they are on an authentic page and give out their sensitive information. Phishing is a type of social engineering. Social engineering is attacks that are with human interaction usually by manipulating the person to perform an action, such as clicking a malicious link or giving out a piece of information that causes a vulnerability in the system.

To fight against phishing attacks, users should be educated in knowing the difference between an authentic website and a phishing one. Also, there are various ways, such as user authentication or network protection based on a blacklist scheme in which incorrect emails are blocked from either the client or server-side [16].

A malicious code attack can be a malicious worm on the internet that small devices with internet connections such as cameras. For example, a worm could infect a self-driving car’s WIFI, take over the system and cause a crash. Botnet Mirai attacks that turn smart devices running on Linux into remotely controlled bots fall under a malicious code attack. An attack becomes a botnet attack when it is done by a single group on multi-connected machines, of which one of them is called a bot and more than one becomes a botnet. The above-mentioned attacks including social engineering are done on the application layer. Mirai can also be used in a DDOS attack in which the attack disrupts the normal function of the device by overwhelming the traffic with requests. [16]

Remote servers, operating systems, and storage servers are usually used in running IoT applications, hence if compromised or there occurs a configuration error, this might cause issues in the application layer.

Keeping the devices in a safe place where unauthorized people may not have access will help protect them from any tampering is another way security could be enhanced. To take the security one notch up, tampering sensors are implemented on the devices and sensors to prevent tampering. Also, the devices should have authorized software and be kept up to date [15]. User authentication should be implemented into the network before it sends and receives any data to make sure that intruders have no access and only authorized users have access to the device. A sub-protocol of IPsec, Ant-replay protocol stops an intruder from making changes to the network package [16].

3.1.2 Attack types on the Perception layer

The following are some of the security issues on the perception layer. It needs even more security compared to the others. The node-level which is a build-up of sensors is one of the favourites for hackers to attack as they can be made use of, and the device software is then replaced with their own. On the perception layer, the devices that have sensors make it possible for outside threats to come in. [16]

A booting attack is when during the start-up process of edge devices, the devices are quite vulnerable to various attacks. This is because the built-in security system does not work during boot-up. This weakness is exploited by attackers. [16]

A side-channel attack is one of the most used techniques to disrupt the protection of an encrypted system. It is another type of information leakage. Power usage, architecture, and sensor devices' way of communication are all ways that reveal information to hackers to allow a side-channel attack. [16]

Noise in data is a threat to a sensor’s data. Having many electrical devices around smart home devices may cause this. The data gets corrupted during wireless transmission due to the wide coverage area making the smart devices receive false or unwanted information which may make the smart home devices act irrationally. AI technique neural network is used in helping to mitigate this type of threat [16]. The way neural network is used is delved into much more detail in the next chapter.

Devices should be connected to reliable networks to prevent a sniffing attack. Encrypting all the data that passes through the network from the smart home devices would level up the security. To prevent the replication of firmware code, a secure boot mechanism is used. Leakage resilient public key that ensures the confidentiality of data is used when a side-channel attack happens and some data is lost. Partitioning and randomization are used to prevent a side-channel attack on the physical level. [16]

3.1.3 Attack types on the Network layer

The integrity and authentication of the data sent to the devices is the main security issue of the network layer.

A man-in-the-middle attack (MITM) might be used to interfere with the communication on a device and its sensor, this kind of attack usually happens between a client and a server. The network traffic could be redirected using

Address Resolution Protocol (ARP) poisoning or changing Domain Name System (DNS) settings. [1]

In MITM, the attacker acts as a proxy between the connections. For example, if an attacker wants to disable the temperature control system of a house, they will target the network between the temperature monitoring device and thermostat, enter wrong data and in this way disable the system. This attack also allows access to other devices in the house as the devices are connected. The current state of the device might reveal to an attacker/robber if the house is occupied or not. Another example of a smart device vulnerable to MITM attack is a smart refrigerator showing a resident's google calendar. This vulnerability is because of the system SSL (secure sockets layer) certificate, which is a problem with IoT devices, allowing the attackers to be able to steal the user's information by using a MITM attack. [1,8]

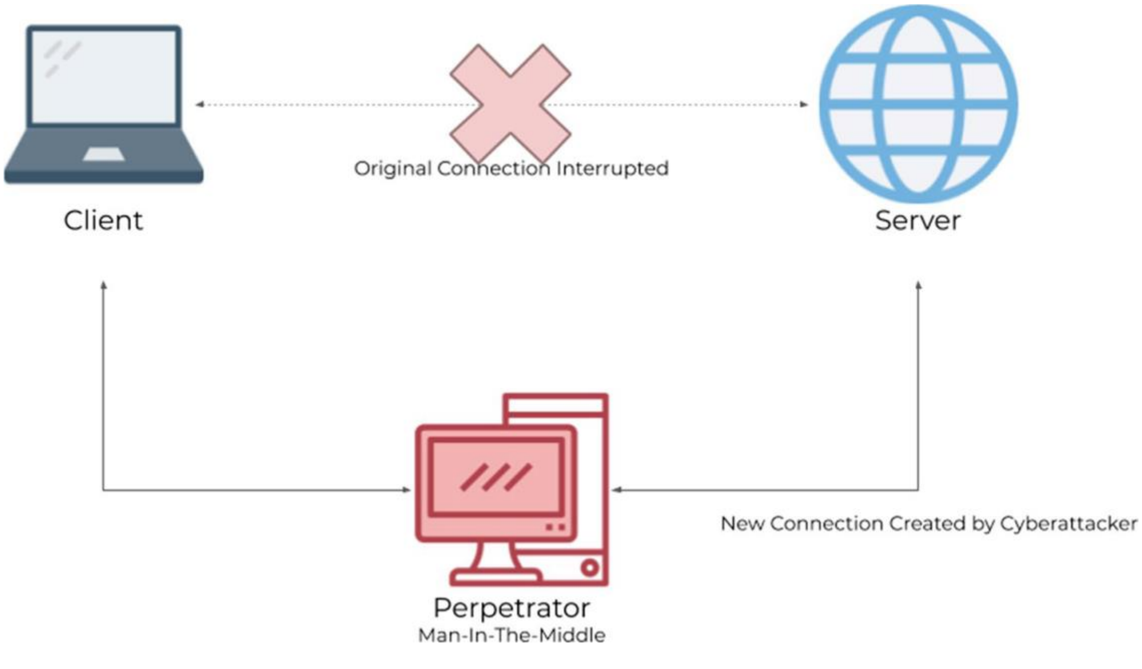

Client
Original Connection Interrupted
Server
New Connection Created by Cyberattacker
Perpetrator
Man-In-The-Middle

Figure 9. A man-in-the-middle attack between a client and a server [1].

IoT has limited computing power and storage and power consumption. This is due to the perception layer consisting of mostly RFIDs and sensors, therefore firewalls should be implemented to filter packets before being sent to the devices [15].

The network layer is also susceptible to a DDoS (Distribution denial of service) attack which is when immense traffic or data is sent to the server or devices and then overwhelmed by the immense traffic. A DoS (Denial of service) is when the traffic is sent by a single machine and a DDoS is when they are sent by multiple machines [1]. A DoS attack makes the user unable to access the network and shuts down the network. The Mirai worm is a famous malware that has been used in some of the largest DDoS attacks. It is designed for IoT devices such as cameras and home routers. The infected devices can then be used in a DDoS attack after becoming part of a wide-range botnet. [1,16]

DOS is countered with an intrusion detection system (IDS) which is a group of tools that detects, monitors, and identifies the attacks and then alerts the responsible person of the attack [26]. An IDS is usually installed on the device or around them, it is usually the first or second line of defence in case of intrusions. IDS system is categorized into two groups, signature-based detection, and anomaly detection. In signature-based detection, the behavioural pattern/signature of the system is compared with already known attack patterns. The behaviour that may be a security threat is saved in the system and the detection system uses it to recognise a bad behaviour by comparing it to already saved patterns/signatures in the system. Because Signature-based detection relies on already known attacks or malware, they are not able to detect new malware. Anomaly detection focuses on normal behaviour. The system decides what normal behaviour is and flags the intrusion activities that vary from the normal behaviour set by a particular threshold. [16,25]

3.1.4 Attack types on the Physical layer

Security issues in the physical layer are mostly physical attacks from either humans or the environment. Examples of some of the security issues are loss of power, hardware failures, physical damages, and environmental attacks. Hence, what is needed to protect the smart home devices in this layer is physical protection [16]. This also prevents tampering attacks. Reverse-engineering also works in countering tampering attacks. Another type of physical attack that could occur is a PDoS (Permanent Denial of Service) attack, this could happen when a smart device is connected to a high voltage power supply and its system gets overloaded making it in need of a replacement [1]. Taking great care of the physical conditions of the devices is extremely important as power is what keeps the device working and alive. Without power, for the device to turn on, all the other layers of the device will be irrelevant.

4 Improving cybersecurity with AI

After looking at the structure of the IoT-based smart homes, what are the common types of cyber security threats and breaches (privacy, phishing, etc.), and where they happen (layers), this chapter focuses on what AI is and how the different types of AI (ML, ANN, Intelligent agents, Computer Vision) can be used to fix the loopholes with the security systems of IoT-based smart homes in order to resolve the incessant threats and attacks as well as the dangers AI in itself poses.

To understand Artificial Intelligence, one needs to understand what Intelligence is. Intelligence is not one-dimensional and can be defined in many ways as people are intelligent in different ways, therefore there is no one way of measuring intelligence. The famous quote, “Intelligence is the ability to adapt to change”, is one of the closest definitions of what Artificial Intelligence is. As AI is not confined by biological methods and is machine-oriented, AI researchers have the freedom to use methods not found in humans. The purpose is to imitate human intelligence and cognitive abilities, not necessarily recreate the human brain. [8]. Using AI to protect a small system might not be feasible as it can be resource-intensive and expensive, however, many of the models are under development and still being researched although, they are not very common and difficult to implement. [1]

There are several traditional security techniques to improve the security in IoT smart homes, such as IDS (Intrusion Detection System), which can be further improved with Artificial Intelligence. As a matter of fact, in cybersecurity, AI is often used in IDS and Intrusion Prevention System (IPS). The two systems work hand in hand, IDS tracks network packets and flags threats detected whilst IPS prevents the detected malicious traffic from being delivered. When implemented together, the system is then called an Intrusion Detection Prevention System (IDPS). [21] The categorisation of IDPS is the same as the explained about IDS in the previous chapter, misuse detection and anomaly detection.

In using AI, the weaknesses in traditional security systems such as low detection rate, slow throughput, lack of scalability and resilience, and lack of automation could be alleviated. Smart home devices are collecting and sending data all the time, which in the case of multiple warnings and alerts, it might overwhelm the teams in large datacentres and security professionals handling them, however, “AI can analyse a huge amount of data and come up with a solution within a reasonable time”. [27] By using AI to help with the prevention of malicious attacks, datacentres wouldn’t have to employ a human security expert around the clock which would decrease the cost. ML assists human cybersecurity experts in the prevention of attacks. Although ML models can work alone, having human supervision increases security and efficiency, and a Hybrid detection model is recommended to use to mitigate threats [21]. There are other categories of AI other machine learning that are very useful in AI cybersecurity such as Intelligent agents and artificial neural networks (ANNs).

4.1 Machine Learning: supervised, unsupervised and reinforced learning

The aim of Machine Learning (ML) is to develop algorithms that learn directly from data, which is akin to how humans learn. As machines can do calculations faster than humans, this makes the methods for them to do intelligent tasks not restrictive. There are different machine learning algorithms, which are Supervised Learning, Unsupervised Learning, and Reinforcement Learning.

A training set or data is needed to build the Machine learning system in Supervised learning. The machine uses this data for learning. This algorithm is an object-pair label pair. The training phase begins when the algorithm is able to decide and learns to recognize the objects by finding the common characteristics and assigning them the right label. The result of this is what is called a machine learning model. [1,8]

There are two categories under supervised learning, classification, and regression. Classification algorithms are used in outlier detection, anomaly detection and novelty detection [1]. The k-Nearest Neighbor (k-NN) is a type of classification algorithm that decides what class a new piece of data should be put in by analysing the Euclidean distance between a new data piece and already classified one to group similar data points. The k-NN technique had been used in detecting false data injection attacks and cybersecurity experts are researching how it can be applied in the real-time detection of cyber-attacks. [1]

A popular supervised learning algorithm is näive Bayes (NB), which is based on the Bayesian theorem which, “seeks to classify data based on the Bayesian theorem wherein anomalous activities are all assumed to originate from independent events instead of one attack”[1]. It is used to forecast whether a class is a normal or attack class. All attributes in NB are assumed to be of equal importance and independent. [20]

Unlike supervised learning, unsupervised learning does not need training data, instead, similarities are identified and grouped in classes and then designated into groups of data coherence and data modularity. This is called clustering and it’s useful in noticing hidden patterns. [8]

4.2 Intelligent agents

Intelligent agents are interactive, decentralised, and autonomous cognitive entity with the goal of taking an action based on their knowledge and the experience it gradually learns from the environment. When used for reconnaissance and exploitation in the target machine, it makes it very difficult to protect against as each agent’s behaviour is shaped by its environment and is different. Agents are used defensively by creating an intelligent agent’s cyber police. The agents are shaped in a cyber environment to malicious acts and issue warnings already in the recon stage as seen in Figure 10.

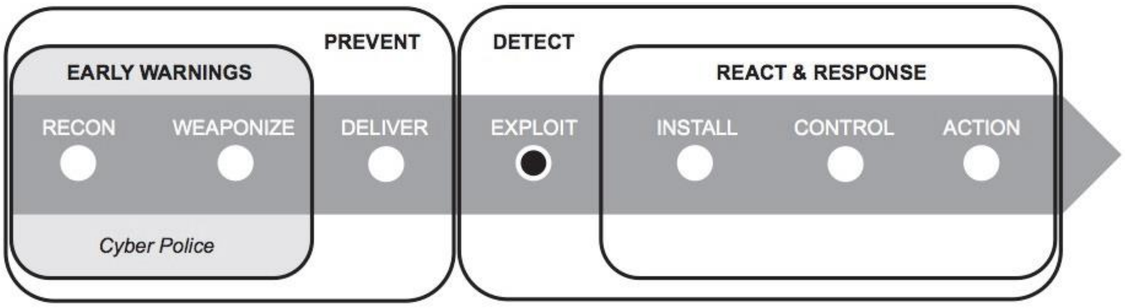


Figure 10. An Intelligent Agent Cyber Police at the beginning of a cyber-attack [27].

4.3 Artificial neural networks

Artificial neural networks (ANNs) are a technique that imitates the way the human brain work, like how the human brain neurons are able to learn from the past and interpret information so does ANNs. They take new information into more serious consideration than the static mathematical model can. [1] Due to this, ANNs are great for monitoring network traffic and thus are used in Intrusion Detecting Prevention Systems (IDPS or IDS) and do well with DoS attacks. It can also be used to eliminate noise in data and be implemented in firewalls for smart homes. The computational effort needed to implement ANNs is a concern in terms of smart homes, however, ANNs were proven to have 90 percent malware detection in advance despite the low computational power. [27]

In the research by Touqueer et al. [16], ANNs are used in pattern recognition and supervised learning. “In pattern recognition, data points of nearest neighbour are compared for noise detection; to remove noise, nearest neighbour algorithms are used. In supervised learning, the neural network is trained against the data that needs to be captured. Then, neural work is deployed to the actual environment” [16]. This is how ANNs work in both pattern recognition and supervised learning. ANNs learn well from past data of network activities and attacks and prevent new ones from happening by being trained using past data. It then identifies abnormal and normal network patterns. This is normally done by security experts but by using ANNs, the time spent doing this task is significantly reduced. [27]

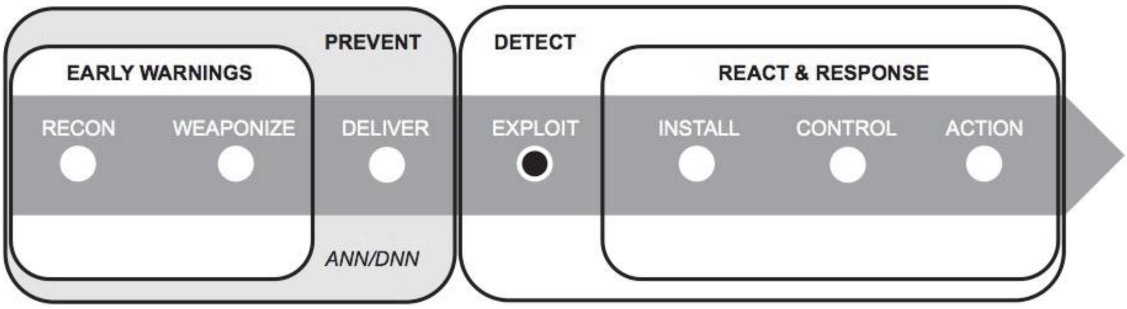


Figure 11. ANN preventing an attack in an ISA [27].

Figure 11 is a cyber kill chain framework within an integrated security approach (ISA) framework depicting when a malicious intrusion can be detected. The cyber kill chain framework follows an attack phase that starts from reconnaissance and ends at action as seen in the figure. ISA framework is a countermeasure to the cyber kill chain phases. As shown in the figure, ANN detects an intrusion at a delivery level, which means it is detected before an attack happens. [27]

Another way that AI could be used for enhancing cyber security is by using the ANNs method in the following research [26]. The research, Defense scheme to protect IoT from cyber attacks using AI principles by Ahanger [26], through its proposed system and evaluation used eight sensor nodes, one server relay node and seven client relay nodes. The sensor nodes adjust their behaviour to the environment. Because the server node interacts with the nodes by analysing, storing records, and replying to the sensor nodes, it is targeted by the attackers. A DoS and DDoS attacks are started in which ten UDP packets are used as attack packets by sending them to the target node, the server relay node, from a single host machine and another ten are sent from four different host machines. The immense traffic overwhelms the target and causes the target node to not be responsive. [26]

Detecting these kinds of attacks at the right time could halt the attacks from reaching the sensor nodes, therefore an ANNs method detection method for detecting DDoS in an IoT network is used. The network was trained with a training set, a testing set, and a validation set using ANN unsupervised and supervised learning procedures. The detection method is based on categorising the normal and abnormal network patterns which were proved to be more than 99% accurate. The method can “detect DDoS and DoS attack during the flow of genuine IoT network traffic” and because of its timely responses, this ANN method helps against network disruptions and improves their performance. [26]

4.4 Computer vision

One way AI can be used to increase safety in a smart home is by monitoring cameras for any abnormalities. This is done by Computer vision. It is a field of study that develops ways for a computer to see, identify, analyse, and understand images as humans do. It uses supervised machine learning methods. [8] Cameras also work as a home security system in a smart home and so do motion sensors. Skin tones, eye colour and other facial and other bodily features are more distinct than other biometrics and thus would be useful in detailed identification. Motion detection and these features would compare patterns learned from movements in the home before alerting owners of any abnormal presence. This identification and classification are done with a convolutional neural networks (CNN) model, which is largely used in image-based problems. [28] Computer vision can be very beneficial to the elderly in a smart home as it can be used to detect abnormalities such as health symptoms, a fallen person or even a change of behaviour pattern by a resident which can then be used to find any oddities as well as prove to be viable security for the residents and smart devices in a smart home. This technique would also be useful in preventing hardware attacks such as tampering.

Disadvantages of AI in Cybersecurity

Although there are advantages to using AI in cyber protection, there are also some disadvantages. AI protections are highly autonomous however they are not fully independent, hence humans and AI systems need to rely on each other to cancel out the disadvantages of each other and increase the reliability and efficiency of the security. [27]

An issue of concern in using AI for threat detection is the occurrence of false positives. False positive is a false alarm, a vulnerability is flagged despite there not being one. The opposite, false negative, also happens whereas threats are not detected despite being present. One way this is combated is to use both human analysts and machines. An example would be the research done by MIT called AI^2 published in the year 2016. AI^2 is an adaptive hybrid platform that first uses AI to go through the data and learn patterns using unsupervised learning. This data is then given to the human analyst who confirms which the real attacks are. The feedback is then included in its models for the next set of data. This has been proven to increase the detection of attacks by 85 percent and the false positives are reduced by five percent. [29]

There have also been other human independent algorithms tested such as the K-means model by Bostani and Sheikhan in 2021, which produced 96.02 percent accuracy and 5.92 percent false positive rate proving that there has been an improvement in the detection by machines alone and although humans are still needed in this area, that might not be so in the future [20].

A notable disadvantage in the application of neural networks to intrusion detection is the “Black box problem” which is an area in neural network research. It is due to the inability of the human brain to understand what method an algorithm is using because the neural network disassembles problems into millions, or billions of pieces and then linearly assemble them[30]. The human brain does not work that way which makes us not know how the machine will continuously act. There have been developments such as SHAPley Additive exPlanations (SHAP) that gives us an insight into which parts of the data input is more important in making decisions. It is visualising tool that makes machine learning models easier to explain by visualising their output. [31]

This field of study is still being developed and researched and Artificial intelligence has the potential to improve cybersecurity by automating the process of detecting and responding to threats. It can also be used to automate the process of analysing large data sets and identifying patterns. In addition, AI can help to ensure that devices are well-configured and optimised for the best performance.

5 Conclusion

The goal of this thesis was to understand what a smart home is, its relevance to the lives of its users, the existing solutions for its growing security and privacy threats and how artificial intelligence is used to improve its cybersecurity. That is, smart homes are beneficial and efficient to have. Smart homes makes a home comfortable and are helpful in aiding in everyday tasks with automation as well as monitoring the wellbeing of the home residents. However, because of how they operate. i.e., by collecting data from the environment of people in the home, there are worries about its security and privacy protection.

There are different types of attacks against smart home devices on every layer of their architecture, ranging from software to hardware, this makes it difficult to have a single solution that will fix all the problems with it. thus the need for further studies in this field. Users can affect the security of the home depending on their actions as they can make a device more vulnerable or safer by being knowledgeable and aware of their devices.

There are different types of attacks against smart home devices on every layer of their architecture, ranging from software to hardware, Users can also affect the security of the home depending on their actions as they can make a device more vulnerable or safer by being knowledgeable and aware of their devices.

Unfortunately, as the usage of IoT devices continues, so will the variety and volume of attacks. Handling these risks using the traditional methods will not be viable in the future, thus the aid of AI techniques is sought. Various AI techniques such as Machine Learning, Intelligent Agents, Computer Vision, and Artificial Neural Networks have been employed in optimising the protection of machines from attacks such as IDS and tampering.

AI is able to analyse a great amount of data hence AI has been proven to be efficient in preventing attacks. The accuracy of threat detection in using AI is proven by research to be faster and more efficient than the traditional methods, especially looking at the massive volume of data and traffic continuously coming in at high velocity. However, it is recommended to have human security professionals in addition to the AI as despite the 90% threat detection accuracy multiple ML and ANN methods produce, they still produce a number of false positives that could easily be resolved with human interventions. Standardising data sets as recommended by security experts will be beneficial in fighting against threats as it will be easier and faster for ML solutions to decode and analyse them [21].

References

1. Kuzlu M, Fair C, Guler O. Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity. Discover Internet of Things. 2021;1(1).

2. Silverio-Fernández M, Renukappa S, Suresh S. What is a smart device? - a conceptualisation within the paradigm of the internet of things. Visualization in Engineering [Internet]. 2018 Dec 1 [cited 2022 Feb 23];6(1):1–10. Available from: https://link.springer.com/articles/10.1186/s40327-018-0063-8

3. Ali B, Awad AI. Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. Sensors 2018, Vol 18, Page 817 [Internet]. 2018 Mar 8 [cited 2022 Feb 13];18(3):817. Available from: https://www.mdpi.com/1424-8220/18/3/817/htm

4. Ghazal B, Al-Khatib K. Smart home automation system for elderly, and handicapped people using XBee. International Journal of Smart Home. 2015;9(4).

5. Darby SJ. Smart technology in the home: time for more clarity. https://doi.org/101080/0961321820171301707 [Internet]. 2017 Jan 2 [cited 2022 Feb 21];46(1):140–7. Available from: https://www.tandfonline.com/doi/abs/10.1080/09613218.2017.1301707

6. Behm R, Uotila E. Smart Homes and In-Home Care for Elderly and People with Disabilities DevOps Metrics-Case Eficode View project Smart Homes and In-Home Care for Elderly and People with Disabilities View project. 2020; Available from: https://www.researchgate.net/publication/348558806

7. Ghayvat H, Mukhopadhyay S, Gui X, Suryadevara N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. Sensors 2015, Vol 15, Pages 10350-10379 [Internet]. 2015 May 4 [cited 2022 Apr

10];15(5):10350–79. Available from: https://www.mdpi.com/1424-8220/15/5/10350/htm

8. Farooq A, Airola A, Heimonen J, Helminen H, Karjalainen N, Laato S, et al. Kurssi: AI & CYBERSECURITY MOOC [Internet]. [cited 2022 Mar 7]. Available from: https://digicampus.fi/course/view.php?id=1391

9. Mare S, Girvin L, Roesner F, Kohno T. Consumer Smart Homes: Where We Are and Where We Need to Go. Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications [Internet]. 2019 [cited 2022 Apr 10]; Available from: https://doi.org/10.1145/3301293.3302371

10. Shenkoya T. Social change: A comparative analysis of the impact of the IoT in Japan, Germany and Australia. Internet of Things (Netherlands). 2020;11.

11. la Ryan Team. IoT and Big Data: Understanding the relationship between these two technologies - Ryax Technologies [Internet]. 2021 [cited 2022 Mar 1]. Available from: https://ryax.tech/iot-and-big-data-understanding-the-relationship-between-these-two-technologies/

12. Sethi P, Sarangi SR. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. 2017;2017.

13. Hübschmann I. An Expert Guide to Actuators in IoT [2021] [Internet]. 2021 [cited 2022 May 27]. Available from: https://www.nabto.com/actuators-in-iot-guide/

14. Sensors and Actuators in IoT | Enabling Industrial Automation - Bridgera [Internet]. [cited 2022 May 27]. Available from: https://bridgera.com/sensors-and-actuators-in-iot/

15. Yousuf T, Mahmoud R, Aloul F, Zualkernan I. Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures. International Journal for Information Security Research. 2015;5(4).

16. Touqeer H, Zaman S, Amin R, Hussain M, Al-Turjman F, Bilal M. Smart home security: challenges, issues and solutions at different IoT layers. Journal of Supercomputing. 2021 Dec 1;77(12):14053–89.

17. 5 Layer Architecture of Internet of Things - GeeksforGeeks [Internet]. 2020 [cited 2022 Mar 27]. Available from: https://www.geeksforgeeks.org/5-layer-architecture-of-internet-of-things/

18. Matin MA, Islam MM. Overview of Wireless Sensor Network. Wireless Sensor Networks - Technology and Protocols [Internet]. 2012 Sep 6 [cited 2022 May 29]; Available from: undefined/state.item.id

19. Usmonov B, Evsutin O, Iskhakov A, Shelupanov A, Iskhakova A, Meshcheryakov R. The cybersecurity in development of IoT embedded technologies. In: 2017 International Conference on Information Science and Communications Technologies, ICISCT 2017. 2017.

20. Kayode Saheed Y, Idris Abiodun A, Misra S, Kristiansen Holone M, Colomo-Palacios R. A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal. 2022;61(12).

21. Zewdie G T, Girma A. IOT SECURITY AND THE ROLE OF AI/ML TO COMBAT EMERGING CYBER THREATS IN CLOUD COMPUTING ENVIRONMENT. Issues In Information Systems. 2020;

22. Zeng E, Mare S, Roesner F, Allen PG. End User Security and Privacy Concerns with Smart Homes End User Security & Privacy Concerns with Smart Homes. 2017 [cited 2022 Feb 13]; Available from: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

23. Jacobsson A, Boldt M, Carlsson B. A risk analysis of a smart home automation system. Future Generation Computer Systems. 2016 Mar 1;56:719–33.

24. Miniwatt Marketing Group. World Internet Users Statistics and 2021 World Population Stats [Internet]. 2021. [cited 2022 Jan 31]. Available from: https://www.internetworldstats.com/stats.htm

25. Bhatele KR, Shrivastava H, Kumari N. The Role of Artificial Intelligence in Cyber Security. In 2019. p. 170–92.

26. Ahanger TA. Defense scheme to protect IoT from cyber attacks using AI principles. International Journal of Computers, Communications and Control. 2018;13(6).

27. Wirkuttis N, Klein H. Artificial Intelligence in Cybersecurity. Vol. 1. 2017.

28. Taiwo O, Ezugwu AE, Oyelade ON, Almutairi MS. Enhanced Intelligent Smart Home Control and Security System Based on Deep Learning Model. Wirel Commun Mob Comput. 2022;2022.

29. Connor-Simmons A. System predicts 85 percent of cyber-attacks using input from human experts | MIT News | Massachusetts Institute of Technology [Internet]. 2016 [cited 2022 Jun 9]. Available from: https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

30. Robbins B. MACHINE LEARNING: How Black is This Beautiful Black Box | by Bruce Robbins | Towards Data Science [Internet]. 2016 [cited 2022 Jun 10]. Available from: https://towardsdatascience.com/machine-learning-how-black-is-this-black-box-f11e4031fdf

31. Verma Y. A Complete Guide to SHAP - SHAPley Additive exPlanations for Practitioners [Internet]. 2021 [cited 2022 Jun 10]. Available from: https://analyticsindiamag.com/a-complete-guide-to-shap-shapley-additive-explanations-for-practitioners/