2022

# A Systematic Study of Data Security Issues in Smart Home IOT Devices

Hilal Nur Issi
*University Of Alabama At Birmingham*

# A SYSTEMATIC STUDY OF DATA SECURITY ISSUES IN SMART HOME IOT DEVICES

by

HILAL NUR ISSI

RAGIB HASAN, COMMITTEE CHAIR
THOMAS GILRAY
SIDHARTH KUMAR

A THESIS

Submitted to the graduate faculty of The University of Alabama at Birmingham,
in partial fulfillment of the requirements for the degree of
Master of Science

BIRMINGHAM, ALABAMA

2022

A SYSTEMATIC STUDY OF DATA SECURITY ISSUES IN SMART HOME IOT DEVICES

HILAL NUR ISSI

COMPUTER SCIENCE

## ABSTRACT

The best description of IoT comes from the International Telecommunication Union (ITU), which defines it as "a global infrastructure for the information society, enabling advanced services by interconnecting things based on existing and evolving interoperable information and communication technologies" (ITU, 2013). Different things, equipment, and household are employed in daily living in our world.

The advantages that smart technology provides have piqued the curiosity of academics and practitioners alike. Home appliances have received a lot of attention, since smart technology has been extensively explored and put into practice. A great deal of research has gone into automating the house, making it accessible via the Internet or mobile phones, conserving energy, assisting older persons with technology, and the most important of all, security. We begin by discussing how the notion of security, especially data security, has evolved in current home automation systems, and then go on to other security concerns in the area.

In this thesis, we will focus on data security related issues in the smart homes. Smart homes detect environments for data collection, transmission, and storage software to ensure privacy and security on the front end while maintaining the quality and availability of the

gathered data on the back end [11]. We need to evaluate, analyze, and compare Smart house IoT security solutions and strategies for data protection to make IoT devices and smart homes more trustworthy. We will conduct a comprehensive research of Smart Home Security concerns, difficulties, and vulnerabilities in this thesis. We'll evaluate and contrast existing data protection solutions, as well as investigate effective new techniques for addressing data security vulnerabilities in Smart Home IoT devices.

The thesis starts with a short working definition of IoT technologies and the Smart Home concept. The literature review is the following part of the thesis. In this part, we focus on the data security issues of IoT-based smart homes. The next part includes a detailed description of IoT security problems. Furthermore, current approaches to these threats are analyzed by comparing and contrasting based on evaluation metrics. Lastly, the thesis includes the conclusion of the current researches comparison.

## DEDICATION

I dedicate this thesis to my parents Namık Kemal ISSI, Nilifer ISSI, and my lovely sister Nazlı Nihal ISSI for their blessings, unconditional love, and support.

## ACKNOWLEDGMENTS

I would like to express my special thanks to my supervisor, Dr. Ragib Hasan. I am grateful for the things I learned from the courses and for his support and guidance throughout thesis. When I have struggled in academic or social life, his support increased my motivation and belief in myself.

I would also like to thank my committee members; Dr. Sidharth Kumar, and Dr. Thomas Gilray. I sincerely thank you for their guidance, advice, encouragement and support in making it a better thesis. This thesis would not have been possible without their valuable comments.

I express my special thanks to my parents Namık Kemal Issi, Nilifer Issi, and my sister Nazlı Nihal Issi. They have been the ones that boosted my motivation in difficult times. I would not have come from an overseas country today and study in the United States as an international student if it wasn't for the support of my family.

Finally, I would like to express my sincere gratitude to the Republic of Turkey Ministry of National Education due to financial and moral support. I would also like to thank the Education Attaché in Consulate General of Turkey in Houston, Prof. Dr. Recai Aydin for his support and guidance.

**TABLE OF CONTENTS**

## LIST OF TABLES

## LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| 6LoWPAN | IPv6 over Low-Power Wireless Personal Area Networks |
| AI | Artificial Intelligence |
| API | Application Programming Interfaces |
| Bluetooth LE | Bluetooth Low Energy |
| CoAP | Constrained Application Protocol |
| DoS | Denial-of-Service |
| EAP | Extensible Authentication Protocol |
| ECC | Elliptic Curve Cryptography |
| EDSA | Embedded Device Security Assurance |
| GPRS | General Packet Radio Service |
| HLSM | Home Localization System for Misplaced Objects |
| ICT | Information and Communication Technology |
| IDC | International Data Corporation |
| IEEE | Institute of Electrical and Electronics Engineers |
| IEC | International Electrotechnical Commission |

| | |
|---|---|
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |
| IoT | Internet of Things |
| ITU | International Telecommunication Union |
| LEAP | Lightweight Extensible Authentication Protocol |
| M2M | Machine-to-machine |
| MIT | Massachusetts Institute of Technology |
| ML | Machine Learning |
| NLP | Natural Language Processing |
| PAN | Personal Area Network |
| PUF | Physical Unclonable Function |
| RFID | Radio Frequency Identification |
| RPL | Routing Protocol for Low-power and Lossy Networks |
| SDN | Software Defined Network |
| SLR | Systematic Literature Review |
| WSNs | Wireless Sensor Network |

# 1. INTRODUCTION

## 1.1.The Internet of Things (IoT)

There has been a rise in the creation of new "smart" devices that can connect to the Internet and be controlled remotely utilizing applications over the last decade. Sensors, software, and the connection of devices together create the Internet of Things (IoT) network.

The Internet of Things (IoT) is set to be the next phase in the information revolution, bringing with it societal change on par with the internet. The IoT is predicted to be massive: by end of the 2020s, 20–50 billion items are expected to be connected as part of the IoT [4], prompting predictions of a US$1.7 trillion investment [6]. As a result, it has attracted the interest of businesses, governments, and citizens all around the world, sparking research in both industry and academia [5,8].

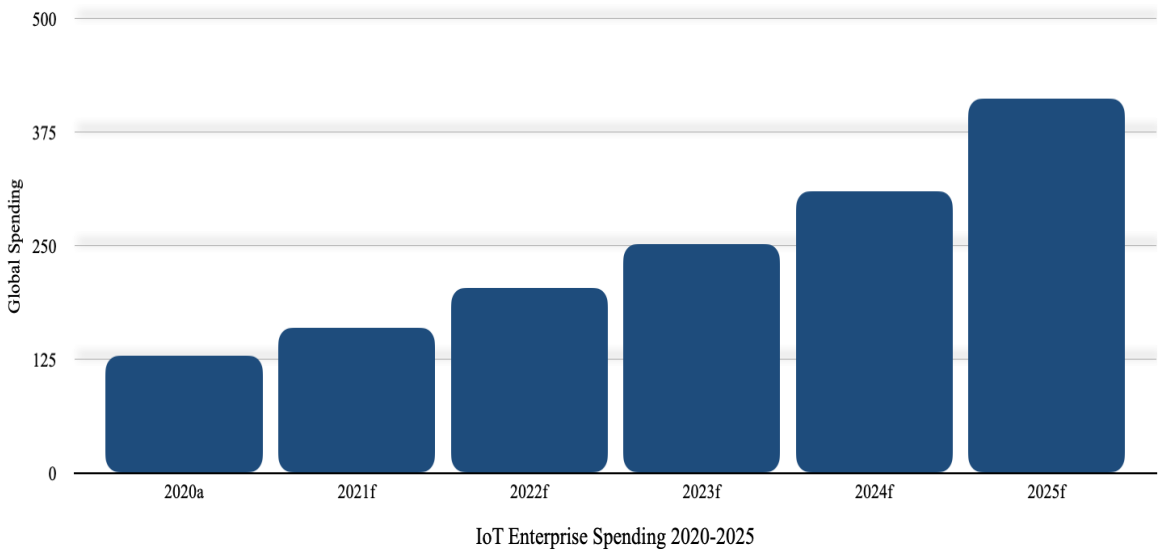


*Figure 1: IoT Growing graph*

In a presentation to Procter & Gamble (P&G) in 1999, Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT), first referenced the internet of things [19]. Ashton named his presentation "That 'Internet of Things' Thing " to embrace the hip new trend of 1999. When Things Start to Think, a book by MIT professor Neil Gershenfeld, was also published in 1999. It didn't use the precise term, but it gave a clear picture of where the Internet of Things was going. The concept of communicating machines was disseminated as a result of these publications, and people became aware of the enormous potential of connected physical items in a digital environment.

Machine-to-machine (M2M) communication, or machines connecting to each other over a network without human contact, gave rise to IoT. Machine-to-machine communication includes collecting data from devices, controlling them, and connecting devices together. The next step of M2M should be able to connect billions of systems, applications, and people inside the one ecosystem while sharing, collecting, and processing

data from the network. IoT is foreseen the next development of M2M because of these reasons. M2M provides the connectivity that makes the Internet of Things possible.

IoT has yet to be given a precise description; nonetheless, it is commonly described as a collaborative ecosystem of context-aware, intelligent, and automated device-connected networks for a specified purpose. IoT is seen as a promising future technology which Gartner, Cisco, and IDC (International Data Corporation), and most companies believe it will be a cornerstone to their next-generation growth power. The Internet of Things, or IoT, consider a network. unique identifiers (UIDs) are assigned for every element of this network, such as people, mechanical and digital machines, animals. With the help of these UIDs, data can transfer without requiring human-to-human or human-to-computer interaction.

The Internet of Things (IoT) is made up of devices that are connected by various communication methods and are integrated with a microcontroller unit (MCU) based systems. Web-enabled smart devices that gather, send, and act on data from their surroundings create an IoT ecosystem. End devices and gateways are the two types of IoT components that are embedded with operating systems. Sensors, devices, and switches are examples of end devices that can only perform a limited set of actions. These devices are typically tiny, have a resource-constrained MCU (energy, ROM, and RAM,) that is highly energy-efficient, and support short-range low-power communication protocols. A more powerful device – the gateway – is required to gather data from these end devices (sensors) or to deliver a command for execution based on an event (devices).

When IoT sensors connect to the IoT gateway or other edge devices in the system, they are able to share their data with the cloud environment or local data management tools.

These sensors are capable of responding to what they receive and communicating with each other. People work on the configuration for the IoT devices and give them instructions to the current system. Then devices work without human interaction.

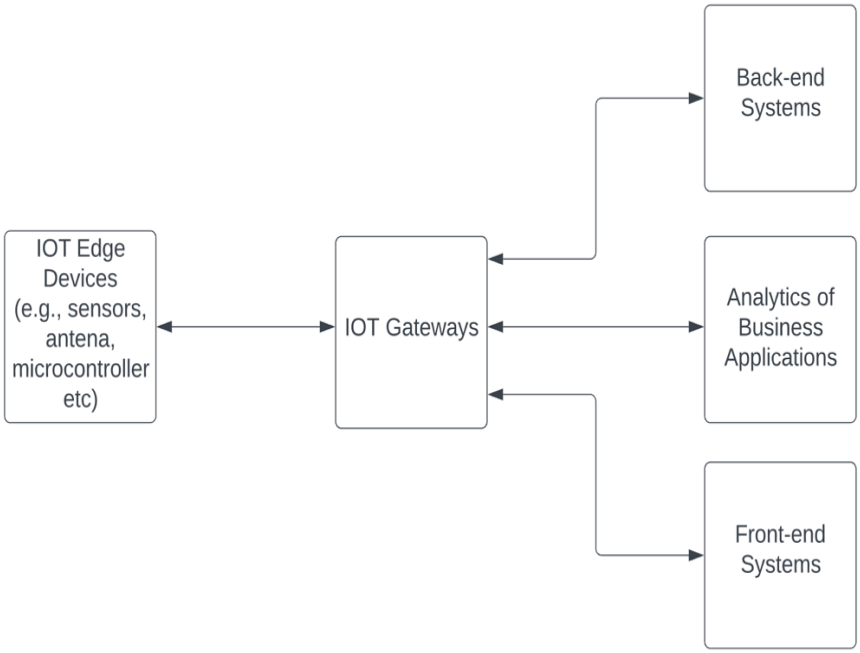


*Figure 2: IoT components communication graph*

Predeployment, ordering, deployment, functioning, and retirement are the primary stages of an IoT device's life cycle, while the work-life cycle of a smart device refers to the process of beginning, initializing, operating, upgrading, and stopping [4].

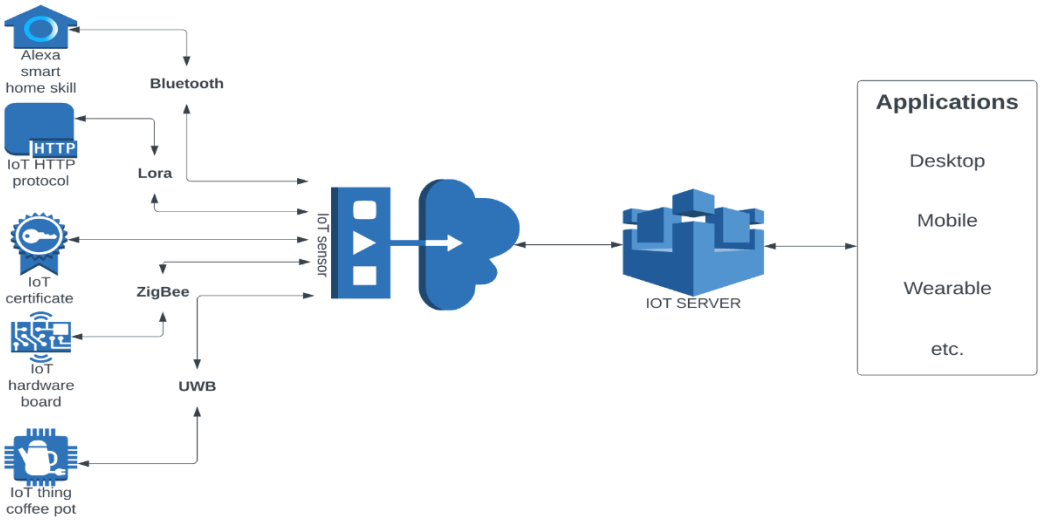


*Figure 3: Workflow for general IoT systems*

IoT devices, low-cost computers, can create data from human reactions. these data can collect and share as a part of mobile applications, big data technologies, and cloud computing. Every interaction between the device-to-device or human-to-device is recorded, monitored, or changed thanks to a hyper-connected environment. Even though digital and physical worlds are collied, they are working together without creating any problems.

The recent years, IoT is consider an innovative technology of smart systems. Communication and connection between devices, people, and processes becoming easy with the help of embedded IoT technologies. The natural or man-made things that are able to use the Internet Protocol (IP) address or transfer data to the network are examples of IoT smart devices. smart cars with built-in sensors to alert the driver when tire pressure is low, healthcare applications such as heart monitor implants, and voice assistants like Amazon Echo and Google Hub are examples of real-world IoT applications. Heterogeneity in the

IoT refers to a wide range of hardware capabilities (such as CPU compute and memory footprint), as well as protocols, platforms, and rules (Figure 3 [26]).

There are several IoT business applications. In practically, there are several marks on the very industry related to smart devices changing the workflow of the current industry. The wide range of applications in this technology comes from its characteristics, being easy to adapt to other technologies while transferring the correct information inside the system. even though it looks suitable to use every scenario, developers should consider the performance of an activity, monitor and regulate at a distance in terms of the environmental conditions. Most technology firms use IoT technologies to make their working process more automated, simpler, and easy to control. Energy companies regard smart energy applications enabled by information and communication technology (ICT) as having potential. Healthcare providers see prospects for sensor networks connected to smart devices that allow the elderly and individuals with chronic diseases to remain in their homes for longer periods of time, with the goal of lowering medical and healthcare expenses. Telecom, cable, and media corporations, as well as hardware and content suppliers, see prospects for transforming the house into a hub for entertainment and gaming. In-home managed IT services are becoming more popular, according to access providers. Security companies see remote surveillance, control, and safety devices as a new business opportunity. Furthermore, it goes without saying that this domain involves a variety of disciplines, as well as different perspectives (e.g. users, system, organization) to identify and study a variety of issues. Voice assistants (Siri and Alexa), wearable fitness and trackers (like smartwatches), IoT healthcare apps, smart cars, and smart home apps are some real-world examples of IoT.

## 1.2. Smart Home

The smart home is a modern application of ubiquitous computing that integrates intelligence into the administration and maintenance of houses for "comfort, healthcare, safety, security, and energy conservation"[1].

The concept of the smart home first arose as a marvel of domestic efficiency in the 1930s vision of "homes of tomorrow" [5]. The majority of promises of "new levels of pleasure, leisure, and luxury," as well as "advantages of modern living with less work on the part of homeowners," were not achieved until the end of the twentieth century. Simultaneously, the focus on residential efficiency shifted to energy efficiency. Darby [2] distinguishes between two types of smart house definitions:

- Smart homes are defined as highly automated residential building with integrated appliances that emphasizes modern technology, convenience, and (domestic) efficiency, with the emphasis on modern technology, convenience, and (domestic) efficiency.
- Building- and system-focused research that focuses on building energy performance, ancillary services, and distributed energy generation, as well as how these issues might be addressed with information and communication technology.

The author Darby [2], goes on to say that both definitions emphasize the importance of communications in connecting devices, enabling remote access and management, and providing services [2]. When discussing smart houses, it's important to evaluate how "smart" and "intelligent" are defined. In the context of universal computing and smart

ecosystems, Edwards and Grinter [6] claim that intelligence has the following four characteristics:

1. Sensor data may be used to evaluate the present status of the world by the environment (e.g. if a motion sensor detector has been triggered, it means there must be someone walking nearby).
2. The environment can infer its present state by considering many elements at the same time (for example, if there are multiple individuals at the table, the system may infer that dinner time is approaching).
3. By examining the scenario from its point of view, the environment may be able to foresee a user's purpose (e.g. if subsequent motion detectors are triggered, it means the user is walking along a corridor, and so the user might want to have their way lighted up).
4. Based on the purpose assumption, the environment may take preventative action (e.g. the system might decide to turn on the lights ahead of time so that the user can walk on their path safely)

Bowes et al. [10] divided smart home technology and telecare systems into four generations, based on the level of technical sophistication, based on the research developed by de Oliveira et al. [19] and Brownsell & Bradley [11]. The category allowed for the progression of smart home technologies and telecare services to be seen.

a. The initial generation of smart home systems were technologies that were activated by occupants' movements rather than artificial intelligence (AI).
b. Basic AI-based gadgets were used in second-generation home technology. Sensors were used to detect changes in the environment, wearable devices were used to

monitor health conditions and identify body inconsistencies, and in-house appliances with built-in function programmers were used to aid in everyday duties.

c. The third generation of home technology signified the period of technological interoperability and multifunctionality, whereas the second generation had stand-alone gadgets. This was made feasible by the addition of voice-activated control and connection with other devices, which allowed data to be captured, processed, and sent inside the network.

d. By 2020, the fourth generation of smart home technology will be in place, with sensors placed beneath the skin replacing existing ones. Brownsell and Hawley [14] proposed these sensors offer a lot of potential for health monitoring and management from a distance.

Devices in a smart home setting must be linked in order to share data. When the environment is able to comprehend the present state of the system, this is referred to as intelligence. For that purpose, many sensors must be able to interact with one another, extending the utility of the data collected. Communication protocols define the methods in which various devices and sensors can communicate. Organizations and coalitions create the standards, hardware requirements, and licenses for these protocols, which determine how information is transferred. According to the mode of propagation, communication protocols are divided into three categories: (1) wired, (2) wireless, and (3) hybrid. The best technology to utilize is determined by the application case. Some protocols have greater ranges, stronger security, and lower power consumption than others. It has led to cloud-centric IoT-based solutions for smart home development [3] when combined with another

new cloud computing technology. This thesis focused on wireless communication protocols. The reason is these protocols are used more than other methods.

There are several IoT communication standards that can be used for different purposes. This thesis explains the most popular protocols that are mostly used in smart home applications.

- 6LoWPAN: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is an open standard created by the Internet Engineering Task Force for (IETF). The 6LoWPAN concept was born out of the belief that "the Internet Protocol could and should be applied even to the tiniest devices,"[3], and that low-power devices with limited computing capabilities should be allowed to participate in the Internet of Things. [4] Encapsulation and header compression algorithms established by the 6LoWPAN group allow IPv6 packets to be delivered and received via IEEE 802.15.4 networks. For local-area networks, metropolitan area networks, and wide-area networks like the Internet, IPv4 and IPv6 are the workhorses for data transport. In the wireless realm, IEEE 802.15.4 devices provide sensing communication capability. The two networks' underlying natures, however, are distinct.
- Bluetooth LE: Bluetooth Low Energy (Bluetooth LE) is a low-power Bluetooth personal area network (PAN) technology developed for Internet-connected equipment and appliances. Bluetooth LE, often known as Bluetooth Smart, was included in the Bluetooth 4.0 standard as a replacement for Bluetooth Classic. Bluetooth LE, like its forerunner, interconnects adjacent devices using frequency hopping wireless technology in the 2.4 GHz unlicensed radio range. Bluetooth LE was first released in 2004 and is now being driven by the fast-growing Internet of

Things (IoT). Bluetooth Low Energy is natively supported by mobile operating systems such as iOS, Android, Windows Phone, and BlackBerry, as well as macOS, Linux, Windows 8, Windows 10, and Windows 11.

¶ Z-Wave: Zensys Inc. created the Z-Wave wireless network. Z-Wave is a home automation-focused wireless communications standard. It's a mesh network that communicates from appliance to appliance using low-energy radio waves. Among other things, Z-Wave may be used to control lighting, heating, air conditioning, appliances, and home security. To deliver Z-Wave signals to a base station, most people utilize a remote control. Z-Wave uses a frequency range of 902 to 928 MHz, which does not interfere with Wi-Fi or other wireless signals. To offer a two-way communication channel, Z-Wave uses a mesh network design. This implies that the remote control device may send messages to electrical equipment throughout the house and get feedback on whether or not the orders were carried out.

¶ ZigBee: Dotdot is a global language for IoT designed by the ZigBee Alliance that allows smart items to communicate and function safely on any network. Zigbee is an IEEE 802.15.4-based specification for a set of high-level communication protocols used to create personal area networks with small, low-power digital radios for applications such as home automation, medical device data collection, and other small-scale projects that require wireless connectivity. As a result, Zigbee is a wireless ad hoc network with low data rate, low power, and near proximity (i.e., personal area). Transmission lengths are limited to 10–100 meters line-of-sight because to its low power consumption, which varies based on power output and

ambient factors. [1] Zigbee devices can send data over vast distances by routing it through a mesh network of intermediary devices.

*Table 1: Wireless communication protocols used in Smart home applications*

| | Wi-Fi 802.11n | Bluetooth | Bluetooth LE | ZigBee | Z-Wave | 6LowPAN |
|---|---|---|---|---|---|---|
| Frequency | 2.4–5.8 GHz | 2.402–2.48 GHz | 2.402–2.48 GHz | 868/915 MHz, 2.4 GHz | 868/915 MHz | 868/921 MHz, 2.4–5 Ghz |
| Data rate | 450 Mbps | 0.7–2.1 Mbps | 2 Mbps | 20/40 kbps, 250 kbps | 10–100 kbps | 10–40 kbps, 250 kbps |
| Range | 10–100 m | 15–20 m | 10–15 m | 10–100 m | 30–50 m | 10–100 m |
| Network size | Thousands (mesh) | 8 | N/A | 65,536 | 232 | 250 |
| Network Topology | Star, tree, P2P, mesh | Star | Star | Star, mesh, cluster tree | Mesh | Star, mesh, P2P |
| Encryption | WPA2 | AES-128 | AES-128 | AES-128 | AES-128 | AES-128 |

A smart house has at least a few gadgets that aren't necessarily smart on their own, such as sensors, appliances, or devices. Moreover, automation does not observe the major picture as it is simply concerning responsible for a small number of things. A sensor creates data but has no actual importance in smart home systems. On the other side, intelligence is characterized as having a wider picture of the entire environment through all of the networked devices and sensors, and therefore being able to better adapt and make predictions based on the present state of the system and past information about the occupants. An environment can only be deemed smart when all data about it is collectively kept and evaluated, patterns extracted, and choices made without the user's interaction. The way devices are consubstantiated, how and where data from sensors and device usage patterns are recorded, how this data is examined and movements are captured, and how the consumer interacts with the devices and vice versa form the framework of a smart home.

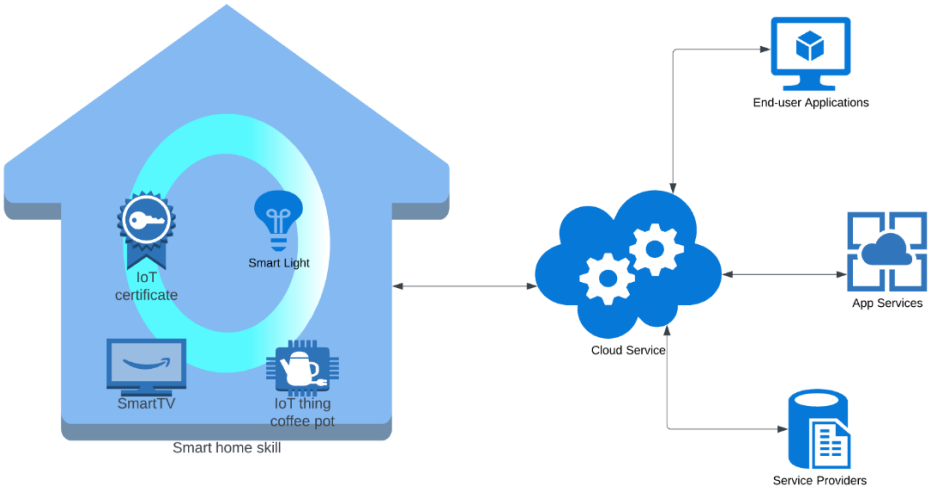


*Figure 4: Traditional Smart home architecture*

Zhou et al. [33] presented CloudThings, a cloud-based architecture targeted at accelerating IoT application development and maintenance. End devices (Things) employ the CoAP protocol in conjunction with 6LowPAN and so have direct Internet connection. CloudThings is an online platform for designing, deploying, maintaining, and assembling Things applications and services that takes advantage of the whole application infrastructure. This structure consists of three parts:

1) Infrastructure as a service (IaaS), which ensures all infrastructure requires in the cloud without the need for concern related to storage, computation power, managing servers, or scalability;
2) Platform as a service (PaaS), which provides a framework for developers to implement, develop and deploy abilities around the things;
3) Software as a service (SaaS), which allows and assists appropriated services such as IoT exploration, data mining, composition, and so on.

For compatibility with end devices, the gateway is often a device that supports various communication protocols. It has enough computing capacity to process data at the network's edge before transmitting it to the cloud. The gateway also ensures a layer of security to the smart home network when it attaches the edge devices to the outside of the systems and authorizes all this traffic to be investigated before commands reach the end devices which have limited resources, lower layers of security requirement, low power. The might essentially give a way to improve availability, dependability, and security while also utilizing increased compute power and scalable design. Third-party service providers working with cloud service providers serve smart home device management, data visualization, and user entry and role management.

A smart house is one that is meant to increase the tenants' quality of life and/or optimize its functioning. In both circumstances, the ability of the system to evaluate and recognize the behaviors of its inhabitants is critical [11]. Thermal cameras, ground pressure sensors, video cameras, radars, and other activity recognition tools are just a few samples. It's critical that activity identification happens in real-time, so the smart home can "respond" and "adapt" quickly if necessary. This is made possible via fog and edge computing. Recognizing and predicting activities is a two-step procedure. The first is activity discovery, which is accomplished by unsupervised learning. The second stage uses supervised learning techniques to recognize and predict activities, which is aided by the clustered data produced in the previous step. If a person entered a room after 10 p.m., laid down in bed, and remained motionless for a period of time, the smart home may presume that the person has gone asleep and turn off the lights and adjust the house temperature to a pleasant resting temperature. The smart house must comprehend and detect human

behaviors in real-time to make this feasible, hence academics are currently working on integrating various methodologies and frameworks to provide activity identification and prediction capabilities to smart homes.

The gradual spread of smart houses and their acceptance by customers is a hurdle in and of itself. To characterize smart home adoption rates, Shin et al. [30] created a technological acceptance model. Compatibility, perceived ease of use, and perceived usefulness are the most important elements in making a purchasing choice, according to their findings. They also claim that senior customers are more likely than younger ones to acquire smart homes. The report finds that a strategy aimed at young customers is essential to boost market demand. The way smart homes are utilized and how they maintain the promises of comfort enhancement, convenience, security, and leisure, as well as energy management, are all closely tied to the issue of client acceptance. Hargreaves et al. [31] conducted a qualitative investigation of the adoption of a variety of smart home devices. The authors highlight four important elements in smart home technology:

1. Technical and social disruption;
2. Household adaptation and familiarization;
3. Learning to use is difficult and there is little assistance; and
4. There is no evidence of significant energy savings and a danger of energy intensification.

## 1.3. Research Statement

In this thesis, we performed a systematic study of Smart Home Security issues, challenges, and vulnerabilities. We compared and contrasted existing solutions for data protection and surveyed efficient new approaches for solving data security issues in Smart Home IoT devices.

The Internet of Things (IoT)applications specifically focus on a smart home are a novel and destructive technology that is mostly unused and messy. We must comprehend the available alternatives and gaps in this field of study in order to give significant insights into technology settings and to assist researchers. Several methodologies have been used to examine IoT-based smart home applications. Current research publications focus on and offer solutions to the barriers that get ahead of the broad use of smart home IoT applications, to the detriment of the category. The field of smart home applications research is ever evolving and diversified.

This thesis provides a concise overview of the underlying issues in IoT data security using research trends and theoretical frameworks. The importance of standardizing the security process has been emphasized as a result of the review of the database.

The research methodology is a means of analyzing approaches in a field of study in a methodical and theoretical manner. This section uses a Systematic Literature Review (SLR) method to provide a clear background on data security approaches in smart homes (Kitchenham et al. [22]; Brereton et al. [11]). In general, the systematic literature review method begins with a statement and continues with an analysis of a specific issue. The research methodology is a means of analyzing approaches in a field of study in a

methodical and theoretical manner. We chose the following research questions to drive our search approach since our major study goal is to investigate research methodologies for verifying the safety of an IoT system that has been compromised due to a security breach:

1. What attempts are being made to assure the safety and security of IoT devices?

2. What program analysis techniques are used to undertake verification and validation?

3. What are the challenges with the implemented or proposed solutions?

4. What are the key takeaways?

This research looks at studies that have been done since 2010. A review is done to create a classification that maps the research environment. We do a concentrated search in three main databases, namely Scopus, Science, Direct, and IEEE Explore, for every paper relevant to Smart Homes Security, IoT Security, Privacy, and Data Security. The initial round of data collection was performed by scanning scholarly resources for purpose keywords. Included are studies that offer a data security evaluation in smart homes.

*Table 2: Number of total studies in the initial round of data collection*

| Topic | Digital Library | Number of Papers |
|---|---|---|
| Smart Home Device Security | IEEE Xplore | 490 |
| | Scopus | 573 |
| | Science Direct | 782 |
| Smart Home Network Security | IEEE Xplore | 445 |
| | Scopus | 843 |
| | Science Direct | 1042 |
| Smart Home Cloud Security | IEEE Xplore | 267 |
| | Scopus | 179 |
| | Science Direct | 678 |
| Smart Home Application Security | IEEE Xplore | 336 |
| | Scopus | 115 |
| | Science Direct | 961 |

In the initial part of our study on databases, we acquired a total of 6711 papers. Keywords were chosen to include the entire range of smart home technology developments related to security issues specifically data security problems, as well as issues such as smart home technology acceptability. The keywords were derived from a larger body of literature and then filtered down to more particular terms (e.g. smart home, IoT, IoT security problems, and Smart home data security issues). An advanced search option was activated during the article extraction process, which confined results to publications in the form of "articles," "book chapters," and "reviews," published in English with keywords. Then we searched the citations of the most significant publications on this subject on Google Scholar for any related and current work in IoT security and safety. To locate any comparable work in a combined domain, a combination of phrases was employed to search the domains of IoT and Security/Safety verification. Examine the abstracts, introductions, and conclusions of the resultant publications to see whether they suggest any relevant technique or

instrument that addresses any of our study goals. Understanding each recommended work to match our study was the final phase.

In the end, we chose 58 articles based on the complete text and the quality of the review to conduct a more extensive and precise analysis. Articles are categorized into four groups. The first category which is on-device security in smart homes covers 9% of the articles. Next category Network security research publications that explore the research state in the security field of IoT-based smart home applications make up 30%. Articles discussing cloud security approaches make up about 20% of the research. In the fourth category, application security in the smart home environment accounts for 41% of the total. Our final study, given in Figure 5, is based on the proportion of selected research publications.

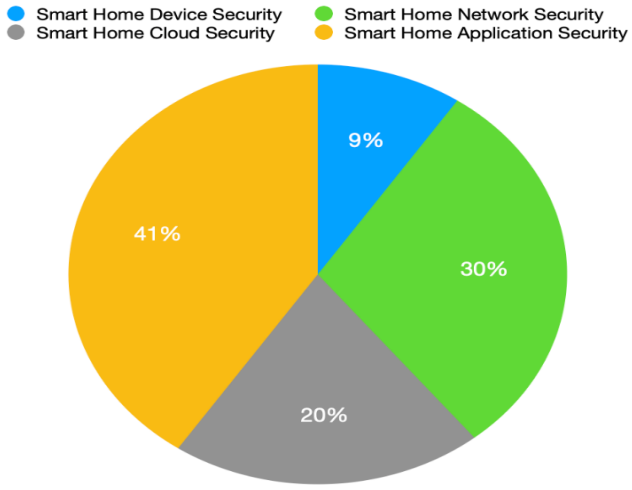


*Figure 5: The ratio of selected research publications*

The review and survey papers describe the present level of knowledge on IoT and smart home security problems. The most recent researches examine the data related issues in IoT smart houses, as well as IoT and its security protocols in smart homes.

Since the data security problems occurred, many security protocols, methods, and architectures are proposed. Screening the literature in the relevant fields provides the opportunity for finding these proposed or implemented security developments. As a result of literature scanning, IoT security problems showed detailed and provides us chances to compare these developments.

IoT security is a popular topic among researchers. So this study collect the common security problems and proposed security solution methods for them on data security in smart homes. Then we compared these proposed solution schemas from researches. While comparing, we are looking at some metrics such as how powerful, how effective to solve problems, and are that suitable for universal usage for all IoT devices. Then, we show the pros and cons of current solutions on data security in smart homes.

### 1.4. Thesis Organization

The rest of the thesis is organized as follows. A detailed literature review was made in Chapter 2. The studies are related to data security issues on IoT-based smart homes. IoT security problems in Chapter 3 are described in detail. Chapter 4 includes information related to data security solutions that come from the literature review. In Chapter 5, we discuss our results from this research and give information related to possible future research areas. Lastly, Chapter 6 finalizes the thesis and provides an understanding into future work that can be applied.

# 2. LITERATURE REVIEW

Since the American Association of House Builders initially announced the notion of Smart Home in 1984, it has been used in a variety of businesses. A variety of e-health projects in the Smart Home sector are discussed by Chan et al. [11]. With the help of technology in the living environment or home, smart homes let the automatic management of equipment and systems in accordance with the construction industry. A number of Smart Houses have been constructed to test smart technology in urban environments. Barlow and Venables [7] gives a rundown of initiatives including mobile applications for Smart Home contexts.

Several research studies have attempted to grasp the technical aspects of the smart home in practice. Over time, the center shifted from the technological opinions of smart homes to the human experience. This has provided a deeper understanding of the ramifications of smart homes in people's lives, necessitating the need to describe the new viewpoint in the evaluation.

“A smart home is an attribute accoutred with sensors that can be monitored, accessed or controlled remotely, and a high-tech network that connects home equipment, devices, and features and provides services that respond to the demands of its residents” Balta-Özkan et al. [13]. De Silva et al. [10] took a similar approach, although they didn't describe the technology aspects of smart houses. It's "a home-like environment with

ambient intelligence and autonomous control, allowing it to adapt to occupants' behavior and supply them with numerous amenities," according to the authors. Balta-Ozkan et al. [13] and De Silva et al. [10] both define automated technology as a means of responding to inhabitants' demands.

Smart homes, as a key component of the Internet of Things (IoT), help consumers by communicating with a variety of IoT-enabled digital gadgets. All smart home gadgets connect with one another in an ideal vision of the wired future. IoT-based smart home technology has revolutionized human existence by allowing everyone to be connected at any time and in any location (Gaikwad et al. [18], Samuel [32]). In the last several years, home automation systems have advanced significantly. These systems offer infrastructure and ways for exchanging various kinds of appliance data and services (Kim et al. [25]). Electricity, sensors, software, and network connectivity within a home is ensured by the Internet of Things (IoT), which is cover the smart home.

Solaimani et al. [34] describe their smart living study. They discovered that Smart Home and e-Health, which place a significant emphasis on technology, are mostly accepted by mono-disciplinary technical magazines. There are also more technical-oriented conferences, which promotes a greater focus on technical topics, experiments, and publications. Their findings revealed that most Smart Home initiatives and trials take place in a research and development setting. The absence of socio-technical and socio-organizational aspects of Smart Home can be explained by the fact that it is currently in the experimental stage. On the other hand, due of technology limitations, smart home concepts are still uncommon. Smart living is prone to developing technological and security-related challenges.

This set of standards emphasizes sustainability and energy efficiency, as well as the potential for smart home services to increase user comfort. Chan et al. [11], focusing on a different environment, emphasized healthcare requirements from the standpoint of elderly consumers. With respect to this statement, a "smart home" is described as "a housing that expectations to ensure affordable home care for an aging population and undefended users". There are also more conceptual reasons that support the notion of smart home technology to satisfy the requirements of the elderly, improve quality of life, and encourage residents' independence (Alam et al. [4]; Blaschke et al. [10]; de Oliveira et al. [19]; Ehrenhard et al. [23]).

Through continuous health monitoring, fully automated devices have the potential to improve residents' quality of life and encourage independent living, especially among the elderly, and they can even give virtual medical aid when needed (Orwat et al. [35]). The combination of smart devices and sensors into a smart system achieves advantages from a variety of economic, social, health, emotional, sustainability, and safety topics, and it provides the management, monitoring, support, and response services benefits.

The difficulty of interoperability across devices employing multiple communication protocols emerges as a result of the heterogeneity of IoT devices present in a smart home. Heterogeneity in the IoT refers to a wide range of hardware capabilities (such as CPU compute and memory footprint), as well as protocols, platforms, and rules. Because low-power devices employ communication methods with small range coverage regions, interoperability between devices is critical. This may be expanded via multi-hop transmission in a mesh-grid architecture. The absence of a common security service is the most serious concern with heterogeneity [12].The issues of achieving network-level

compatibility across different technologies are discussed by Bello and Zeadally [7], who use the 6LowPAN protocol as a middle ground solution.

To put it another way, the smart home's design specifies the services and advantages it wants to give (Chan et al. [11]). When it comes to lifestyle assistance, a smart home means a home equipped with domestic equipment and sensors attached through a communication network. It allows users to operate domestic equipment remotely, reducing the time spent on mundane household tasks (Chan et al. [11]; Amiribesheli et al. [5]). Residents of smart homes may use connected gadgets to better monitor their energy use while also improving their convenience and comfort in their everyday lives (Scott [35]).

Pilloni et al. [32] focus on the energy efficiency component of smart home development and present the occupant-perceived quality of experience idea (QoE). The authors next suggest a QoE-aware smart home energy management system (EMS) that bases its energy savings on the level of discomfort produced by changes in appliance operations. Zhang and Musilek [29] utilize pain measures to promote long-term, active engagement in demand control programs.

The key function that a smart home delivers, according to Reinisch et al. [32] and Scott [34], is energy usage control. Reinisch et al. [32] see an intelligent house as a collection of gadgets that work together as a single system to monitor electronic appliances, encourage effective energy management, and promote sustainability. The service is made possible by the integration of technology components such as smart heating and smart meters, according to Scott [34].

Risteska-Stojkoska and Trivodaliev [33] outline a variety of difficulties and solutions for IoT-based smart houses. The authors emphasize the need of optimizing communication among Smart House devices in the field of edge (fog) computing, suggesting the creation of lightweight algorithms for local data processing and lowering the number of transfers between devices. As a result of the large volumes of data created by the devices, new big data technologies for integration, storage, and analysis are required. Distributed data processing systems, NoSQL databases, and business intelligence platforms are all possible possibilities.

Chan et al. [11] were to address the technological status of diversified smart home efforts and provide a full comprehension of the current and future challenges that smart homes and smart technologies pose to consumers. The authors criticized the prevalent practice of highlighting technology's potential benefits while ignoring users' perspectives and adopting a product-centric approach. They claim that the existing technical specialization in the study reflects the market's lack of adoption of smart homes.

To operate in real-time, smart systems require a reliable communication and computation infrastructure that allows for data interchange and intelligent decision-making. Decentralized security and anonymity are provided by blockchain-based techniques [31], but at a significant energy and computing expense. Dorri et al. [9] presented a lightweight blockchain instantiation that is specifically designed for IoT-based smart homes. The authors demonstrated that increased security and privacy may be achieved with minimal traffic, processing time, or energy use (Framework for transitive energy).

Automation, mobility, and interoperability of technology are seen to be adoption enablers (Yang et al. [48]). Furthermore, the usability barrier, which refers to the dependability and simplicity of use, has been found to play a critical part in the adoption of smart home technology, with the complexity of the technology leading to a refusal to use it (Balta-Ozkan et al. [13]; Alsulami & Atkins [8]). However, a lot of smart home gadgets on the market today are difficult to operate. The user's perspective on ease of use was under-researched because the bulk of smart home initiatives were entirely technical in nature (de Oliveira et al. [19]; Diegel [24]).

The low rate of perceived utility of smart homes, according to Balta-Ozkan et al. [13] and Kerbler [15], can be explained by a lack of understanding, trust, and experience in embracing the technology's benefits. People aren't entirely aware of the operations, hazards, and advantages of smart home devices since they're new. Lack of awareness of smart house technology, according to Balta-Ozkan et al. [13], is impeding the widespread adoption of smart homes in the general market. The input of technology adopters, which may not always be favorable, has a significant impact on how emergent technologies are perceived (Hu et al. [35]). As a result, a lack of user knowledge combined with unfavorable word-of-mouth might have a detrimental impact on potential consumers' adoption of smart home technology (Yang et al. [48]).

In the context of a smart home, security is largely concerned with data security and privacy, as well as safeguarding the privacy of the residents. Physical security and safety (for example, against natural elements or unauthorized entrance) are equally critical, although they are beyond the purview of this assessment. Security must address the following challenges, according to Zheng et al. [43]: 1. Preventing data breaches (ensuring

that unauthorized entities are unable to access the data); 2. Authorization (defining who has access to the data); 3. User privacy.

The dependability factor refers to the technology's capacity to service consumers for an extended period of time, with a normal product lifespan of at least 5 to 10 years (Balta-Ozkan et al. [13]). Smart homes are expected to understand users' requirements and give personalized support (Kim & Shcherbakova [38]). People, on the other hand, were found to be typically suspicious of smart home devices' dependability (Balta-Ozkan et al. [13]). Given that smart homes are becoming more mainstream, it's critical to assure user safety and security.

*Table 3: Comparison of existent methods on the smart home security*

| Research | Characteristics | IoT Network | Cloud | User | Attacker | Service | Platform |
|---|---|---|---|---|---|---|---|
| | *Heterogeneity, Resource Constraint, Dynamic Environment* | *Privacy, Multicasting, Bootstrapping* | *Availability, Data Protection* | *Social Engineering* | *Threat, Control System Security* | *Trust, Access Control (Authentication, Authorization), Middleware* | *Security Service based on Security Level, Self-verification* |
| Alqassem [21] | Heterogeneity | Privacy | - | - | - | - | - |
| Lee et al. [22] | Heterogeneity | Privacy | - | - | Threat, Control System Security | Access Control | - |
| Aomhara et al. [23] | Resource Constraint | Privacy | - | - | Threat | Trust, Access Control | - |
| Huang et al. [24] | - | Privacy | - | - | - | Access Control | - |
| Alqassem et al. [25] | - | Privacy | - | - | Threat | Access Control | - |
| Kim et al. [26] | Resource Constraint | Privacy | - | - | Threat, Control System Security | - | - |
| Li et al. [27] | Heterogeneity | Privacy | - | - | Threat | Trust, Access Control | - |
| Rahman et al. [28] | - | Privacy | Data Protection | - | Threat | Access Control | - |
| Proposed | Heterogeneity, Resource Constraint, Dynamic Environment | Privacy, Multicasting, Bootstrapping | Availability, Data Protection | Social Engineering | Threat, Control System Security | Trust, Access Control, Middleware | Security Service based on Security Level, Self-verification |

Magruk [39] demonstrates how selection criteria are used to assess the obstacles of IoT and cloud computing paradigm integration in smart homes. The data collection process can be done by using Artificial intelligence (AI) and machine learning in the IoT systems. With the help of these methods, this process becomes simpler and more dynamic.

Other works are divided into separate groups depending on the security activities and efficiency in IoT-based smart home systems. These studies glance at secure data management on diverse applications, security frameworks and applications for smart homes using IoT, network system privacy and security control for smart homes, and security extension in smart home systems and applications (Sanchez et al. [46]). Another topic of discussion is safe healthcare architecture (Moosavi et al. [44]) and node communication in a Constrained Application Protocol (CoAP) network (Bergmann et al. [12]), as well as security difficulties in smart homes between diverse devices and apps (Arabo [9], Lee et al. [32]).

Inside the smart home security issues, secure software updates on IoT devices; security system devices (e.g., CCTVs), and password security and applications (Shivraj et al. [37]) are important subtopics researchers looked at. Schiefer [38] defines threats to home automation and security in his research. A new strategy for risk minimization is presented in case of privacy breaches in smart energy management systems. Jiang et al. [29] research article highlights machine-to-machine technology development and deployment in smart homes and security systems.

# 3. IOT SECURITY PROBLEMS

Chan et al. [10] said without widespread computing and a plethora of sensors strewn throughout a home, the notion of a smart home would not have been viable. Unfortunately, the usage of these gadgets, which are often connected to the Internet (directly or indirectly) and/or employ wireless communication, opens up new avenues for assaults on the security and privacy of those who live in the smart home.

Jacobsson. et al. [28] explained that identifying an intruder attempting to gain access to the home, alerting the homeowner about the intrusion or intrusion attempt, preventing the intruder from gaining access to the home, and gathering or collecting evidence regarding the intrusion so that the perpetrators can be brought to justice are just a few of the tasks of a modern security system. The evolving perception of security in modern households has been aided by technological advancements. It has progressed from a basic lock and key security idea to the use of complex security systems that include cameras, microphones, contact sensors, proximity sensors, alarms, quiet alarms, and other features.

The main barriers to modern home automation systems, according to A.J. Brush et al. [9] the high total cost of the system, lack of the right devices at home, lack of resilience due to the integration of various devices into smart home systems, complex user interfaces and confidence on talented supervisors. All of these aspects contribute to a lack of manageability and compelling security.

According to C. Karlof and D. Wagner [18], commonly used technologies and networks for home automation have several risks. They look at a variety of wireless sensor network routing attacks (WSNs). Sinkhole attacks, Selective Forwarding attacks, Sybil attacks, and Cloned ID assaults are all examples of this. Y.C Hu et al. [21] discovered a Wormhole attack on wireless networks in 2006, in which the attacker collects data packets in the network at one point, tunnels them to another site, and then retransmits them to the network. Even though all conversations in the network are done with secrecy and integrity using IP sec in 6LoWPAN, this attack may be carried out.

Almost all wireless encryption protocols now specify data packet integrity, device authenticity, key setup, and encryption requirements. J. Wright et al. [20] demonstrated how replay attacks may be used to exploit ZigBee or 802.15.4 wireless networks in 2011. The new key is broadcast over the air in plain text during reflating. An attacker can use this to sniff for encryption keys in plain text, inject, decode, and change data packets, all of which can be used to influence a device's operations. B. Fouladi and S. Ghanoun [22] demonstrated a weakness in Z-Wave door locks in 2013, allowing an attacker to get complete access without authorization.

T. Oluwafemi et al. [43] shown how a basic item in a house, such as a fluorescent light (CFL), linked to a home automation network or the Internet, may be managed to inflict bodily harm to a home's residents. Furthermore, for persons with photosensitive epilepsy, lights changing at specific frequencies might be extremely harmful [24]. When a home automation network is connected to the Internet, an attacker may be able to obtain control over switches and dimmers, as well as devices plugged into power outlets.

Individuals may live in secure settings thanks to smart houses. Smart mobile homes can notify people about potentially dangerous actions (Bao et al., 2014). In sensor networks, wireless sensor networks should be a safety issue. Sensor nodes are simple to modify. Li et al. [27] mentioned that this sensor network architecture has issues with data establishment and data management process. Because this network is easy to manipulate, data from this network is critical for smart home reliability. Nodes are encrypted to provide end-to-end security. However, because IoT systems are heterogeneous, certain nodes may be able to incorporate general-purpose microprocessors. Low-resource and limited devices, on the other hand, can only integrate application-specific ICs [6]. Due to its compact size, limited power supply, low computing power, limited memory, and limited battery life, traditional cryptographic primitives are not convenient for low-resource smart devices.

Due to the variety of the devices and protocols, as well as the scale or number of nodes in the system, implementing security methods in an IoT system is more difficult than in a typical network.

Kim et al. [6] defined that several types of IoT devices and look at the security risks that each one poses. In Kim's work, he looked at data protection, device identification and authorization, communication security, device monitoring and control, physical security, and the constitution of lightweight protocols and encryption techniques topics. Li et al. [27] investigate security issues using a tiered architecture that includes sensor, network, service, and application layers.

Interoperability is harmed by heterogeneity, which results in extra expenses for performance and money to interpret each other [7]. Making security-related rules and upgrades is also more difficult. Some technologies (e.g., Meta data registry (MDR),

middleware) can be used to overcome these challenges, but they are not a fundamental answer.

Sensitive data (e.g., home CCTV footage, personal location, and health information) can be utilized to help individuals in some instances. Some smart house apps and procedures may jeopardize occupants' safety. Sending incorrect information to users is one example. Such situations affect the decision-making process. To prevent implementing actions that jeopardize safety, proper processes must be followed (Neisse et al., 2015). IoT devices typically use the cloud because their low memory capacity prevents them from storing data locally. IoT devices, on the other hand, cannot preserve data if the cloud is down for whatever reason.

Insecure web and cloud interfaces are application layer vulnerabilities that might be used to attack an IoT system. As a result, security measures on cloud gateways are required to prevent malicious actors from altering settings.

Another critical issue is one of storage. The cloud environment should guarantee data storage confidentiality and integrity [8]. However, the natural vulnerabilities of cloud environment make the data confidentiality and integrity is an important security topic for cloud IOT applications.

There are several studies on data integrity and confidentiality in IoT data, but the most of them are focused on data on the cloud. We saw that there were still some gaps in this area, so we chose to look at data privacy security in IoT data contexts.

### 3.1. Data Management Security Problems

The Internet of Things (IoT) is becoming more and more common in the human experience. It may be used with anything, anywhere, at any time. From 'smart' automobiles that interact with each other and vacuum cleaners that produce blueprints of homes to watches that count calories burned and light bulbs controlled via the Internet, the Internet of Things (IoT) is now entwined in everyday life. Its pervasiveness also indicates that all data collected or processed by IoT devices may be used to make conclusions about human behavior and preferences, either directly or indirectly. While some may see the benefits of these inferences, such as tailored services, others may be concerned about the ramifications of their personal data being collected and used.

Data can originate from one of three places in a smart home: passive interaction with the user (wearable body sensors, motion detector sensors, RFID identification tags, smart floor sensors, silhouettes from depth cameras, and video from cameras), active engagement with the user (gesture identification, voice commands, interacting with a touch screen, detecting actions by pressing a button), or non-user created sources (thermostat readings, and air flow sensors).

Chan et al. [10] defined smart grid environment in their research. CCTV systems will be installed throughout the city and sensors will transmit all collected data to the network. Big data will also diversify the sorts of information available and eventually expand the amount of data available. The importance of maintaining privacy in this scenario cannot be overstated. Researches must conduct future search on security for privacy while keeping in mind the features and security requirements of IoT.

IoT security systems are still in the works. Despite the widespread use of surveillance and image processing to solve concerns connected to safety and surveillance in smart homes, services for the elderly may be unavailable due to the lack of a safety system (Mano et al., 2016). This study showed that surveillance data from smart homes are vulnerable to the data transferring process and can manipulate with attackers. Because of this reason they make users' privacy can be bypassed.

Ganz et al. [34], and Bergmann et al. [15], uncertainty can be ascribed to faulty data resources (e.g., erroneous sensor readings or unreliable external environment data collecting networks) or the inability to discern whether a phenomena has happened based on existing information. Data loss occurs as a result of these issues in smart home devices.

Several researchers are concerned about data flow across heterogeneous devices, as well as the possibility of electrical hardware failures in IoT-based smart homes, which might result in significant data loss ([15], [17], and [18]). Home automation systems are burdened by the flow of massive volumes of data and complicated control ([5], [11], [14], [27], and [33]). Many smart home gadgets that can exchange data and be managed over the Internet might be vulnerable to a variety of assaults; hackers could try to remotely manipulate equipment, steal personal data, or modify the contents of messages while they are being transmitted [3]. Waltari and Kangasharju [40] found that when huge volumes of private data flow through smart home devices, data can be lost during the connecting process unless the data is adequately regulated and according to the wishes of residents.

Li et al. [27] found that various obstacles inhibit efficient data transport in IoT-based smart home devices. Data theft is defined as intercepting data packets and tapping lines to steal transferred information and data between a terminal host and a home gateway.

A hacker attaches a virus to a data packet and sends it to the system during a viral attack. Through continual self-replication, the virus consumes system resources. The most recent DoS assaults entail arranging massive volumes of data in order to simultaneously reach several home gateways. The server is unable to check the validity of users, execute normal data access, or fulfill its job. An attacker alters stolen data and delivers an error message to a home gateway or end hosts while illegally processing user data.

Sun et al. [37] explained that because a home gateway system works with heterogeneous sensors spread throughout a home environment, highlighted that it faces various challenges. When a failed transmission of a network system's test data is used in ZigBee wireless data transfer, for example, the network system's data loss rate is 0.4 percent; when a user in a smart home begins remote video monitoring, the system loss rate is roughly 7.6 percent (Han et al. [27], and Sezer et al. [29]).

Data management security has been highlighted as one of the most critical barriers to establishing energy-efficient smart houses in IoT contexts. The dangers of using and potentially misusing information regarding properties must be acknowledged. In the absence of a security system, the dangers connected with the usage, possible misuse, and exploitation of information about residences are increased, resulting in increased energy consumption ([23], [27], [28], [34], [37], and [42]).

The Internet of Things introduces security challenges, such as authentication, and access control, which must all be classified. In smart houses, security applications must be implemented. Techniques for security operations are the subject of research (Elkhodr et al. [11]). One of the most significant challenges to smart home automation is a lack of security in IoT contexts. When motion and environmental detectors detect unusual situations,

inhabitants are notified by phone or the Internet, and surveillance cameras in all sensitive locations are activated (Kirkham et al. [25], Jacobsson et al., [20]). The security of a smart home's whole infrastructure is primarily reliant on security systems; security system failures can cause a home to malfunction (Min and Varadharajan, [29]). Problems with energy data in smart homes lead lights to switch out, and smart gadgets that are integrated in the scheme of things become open to assaults [15].

The hazards posed by these technologies are frightening. In today's buildings, a variety of sophisticated network devices have inadequate security capabilities or none at all. As a result, these devices are readily targeted by prospective attackers, posing a threat to the safety of building residents and disrupting the normal working of whole structures (Magruk [27]).

IoT privacy and security concerns are expected to be more pressing than they are on the Internet. Individuals' safety can be influenced by IoT devices if a malicious attacker takes control or provides incorrect information to damage their decision-making process. To avoid the execution of activities that compromise safety, a tool or system that enforces regulations for IoT devices is required (Gaikwad et al. [16], Cebrat [9]). As a result, security solutions are critical to secure data and medical information in smart homes because some attackers modify data [11].

The use of IoT in smart homes opens the door for hostile actors to launch attacks that directly harm smart house users. Sniffing operation methods, CCTV systems, and DoS assaults are all security problems [30]. Accidents in security and reaction time can result in catastrophic failure on the Internet, resulting in a network's communication being disrupted or its speed being slowed [18].

Han et al. [34] defined that data leakage pose a variety of issues in smart homes. As a result, in an IoT context, security vulnerabilities must be considered. Some smart home equipment are insecure and lack sufficient data encryption or authentication, making them vulnerable to DoS attacks, man-in-the-middle assaults, and other malicious vulnerabilities that jeopardize residents' connectivity and physical security. Around 27% of Wi-Fi networks in London are either inadequately protected or not secured at all [44]. Intelligent mobile home systems employ wireless connection to operate household devices via mobile smartphones. In smart homes, security threats such as unauthorized mobile access by hackers may exist. Bao et al. [5] showed because hackers may listen in on conversations, security concerns may also be linked to privacy concerns. The packet forwarding path of IoT devices in the systems of the smart home uses connectionless routing. Because of the lack of a security mechanism, packet loss transmission might occur due to incorrect channels, unprotected wireless communication channels, collisions, and delays [29].

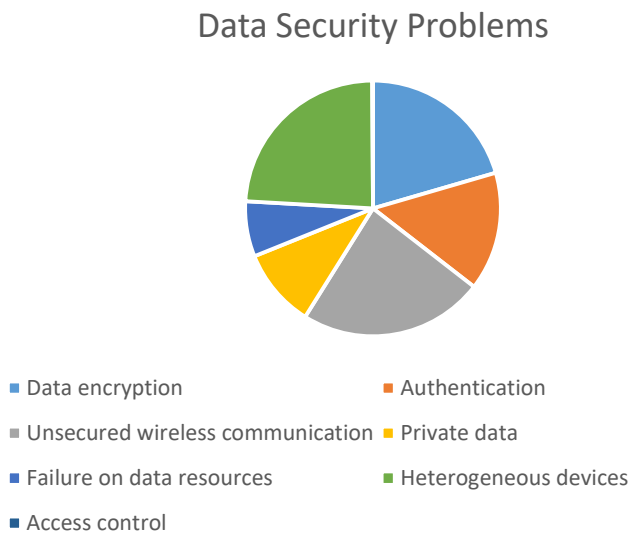


*Figure 6: Data security problems in the Smart home IoT*

In our research, we focus on data security problems. Figure 6 summarized the Data security problems in the IoT based Smart homes. As the figure showed the main reason for data security issues is coming from the heterogeneity of the IoT devices in smart homes. Researchers found that the heterogeneity of IoT devices creates some vulnerable points for systems. Another point is unsecured wireless network channels. IoT devices are less capable in terms of storage capacity. Because current secure wireless network channels protocols required more storage and processing capacity, this topic is still popular among IoT security researchers. The next problem in the Figure 6 is the data encryption problem. The place where data s occur and processes are generally the different places. When data occur, data should move to a place, which is cloud systems generally, to process or store. But the moving data from one place to another place should be secure. If data can be encrypted before transferring, it makes the system more secure. But cryptography mechanisms require more power than IoT devices are capable of. Furthermore, Authentication mechanisms for IoT devices, loss of Private data from the smart home systems, and failure on creating data from IoT sources are commonly discussed topics on IoT security.

Smart home environments are vulnerable to third party attacks. The literature review showed that researchers are focused on three main parts in the smart home data security topic.

- Network related problems:

  Data encryption, Authentication, Unsecured wireless communication, Packet loss on transmission

  DoS attacks, Man-in-the-middle attacks, Unauthorized mobile access, Eavesdrop

- IOT architecture related problems:

  Heterogeneous devices, Failure on data resources, Home gateway viruses

  Lack of common security protocols

- IOT work flow related problems:

  Incorrect information to damage their decision-making process, Reaction time delays,

  Less monitoring ability of attackers “footprinting”

Families are made up of people of varying ages who behave in a variety of ways. An attacker who compromises a home automation network, unlike any other cybersecurity breach, can cause a wide range of consequences, including physical harm to residents, emotional harm, permanent damage to electronic devices, loss of reputation, financial damages, environmental damages, granting unauthorized access to anyone, theft, blackmail, vandalism, or voyeurism, to name a few.

# 4. DATA SECURITY SOLUTIONS

Internal assaults are conceivable when the cybercriminal is near the residence, but external attacks are possible when the cybercriminal has access to the Internet. Although the Internet of Things (IoT) provides significant advantages compare to traditional communication technologies in terms of smart home applications, these applications are still vulnerable to security assaults. In accordance with a recent HP study [51], 80 percent of smart home IoT emplacements breach the privacy of personal information which are last name, gender, marital status, etc. Again, in the same context, more than 80 percent are unable to request passwords of sufficient length and complexity, and 60% have safety and security failures in their user interfaces [6], [7]. In either case, the attacker wants to get into the smart home's infrastructure or obtain access to data saved on cloud services. For example; Eavesdropping, Impersonation, Software exploitation, Denial of service, Ransomware. This section related to the proposed solution to prevent attackers to get the access of the smart homes.

Figure 7 depicts the prevalence of web searches for the phrases Internet of Things, Smart Grid, and Smart Home security problems from 2004 [52]. According to Google's data, the phrases privacy and security on the Internet of Things and Smart Home will continue to rise in popularity.

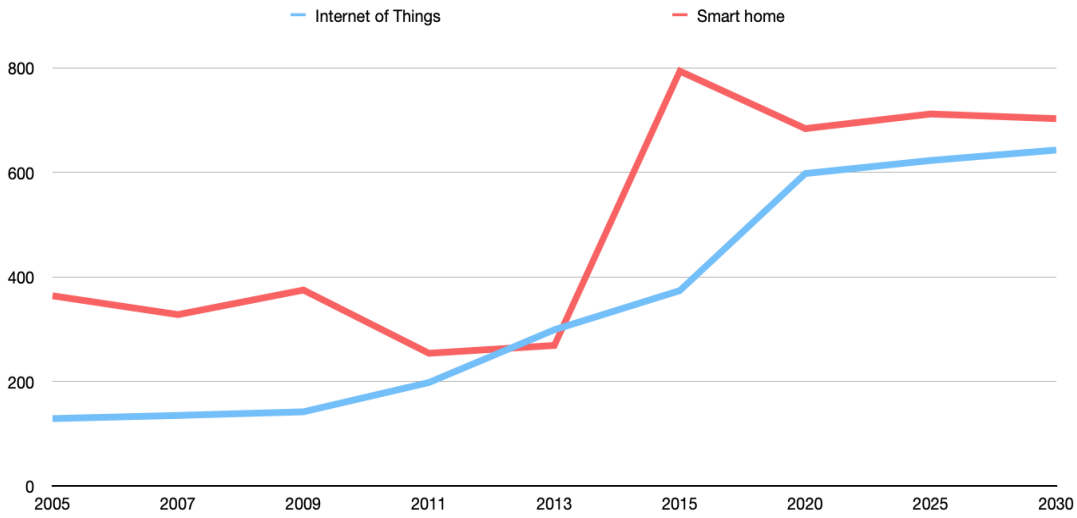


*Figure 7: Attention to phrases Internet of Things, Smart Grid, and Smart Home security problems*

Researchers have established techniques to investigate the cybersecurity of network, like the Assessment Assurance Level with Common Criteria certification based on ISO 15408 [17] and EDSA (Embedded Device Security Assurance) certification comes from IEC 62443 [18]. Moreover, these references are highly professional. IEC 62443 is specifically designed for crucial infrastructure in industrial management systems. ISO 15408 focuses on standard guaranteed and does not specify which attempts to receive. Furthermore, neither method provides an easy way to describe the level of cybersecurity in IoT goods (for suppliers and/or non-security-savvy users).

A context-aware home automation system aims to understand the situation in which a user makes a decision. Predicting a user's location inside the house helps to define the context. B.N. Schilit et al. [28] outlines many ways for determining a user's position at home. The research suggests the use of an infrared grid to properly forecast the user's location in the home, resulting in increased security. This might boost security tremendously, but it is cumbersome for the user. B.N. Schilit et al. [28] concludes that, rather than the system making context-aware judgments on its own, smart home technology

should aid residents in making energy-saving or security-conscious decisions by notifying or reminding them when such an opportunity occurs.

Another approach for IoT security developed by Yin et al., 2015. They developed IoT-centralized management approach for smart houses. A mobile smart house concept has been developed and implemented by Bao et al. [11]. To characterize the effectiveness of human interactions in smart home applications, a model based on a fundamental mathematical method is designed and deployed.

### 4.1. Secured IoT Smart Home Architecture

For a secure IoT environment, B V Santhosh Krishna and T Gnanasekaran [51] provide the most common secure IoT architecture. Other researches generally focus on only one part of this architecture. In this thesis, we will use this architecture as a baseline for IoT based smart home architecture and collect and discuss the other researches inside the corresponding layer.

IoT must guarantee that all levels are secure. In addition, IoT security must wrap the overall system, including the perception layer, network layer, middleware layer, and application layer.

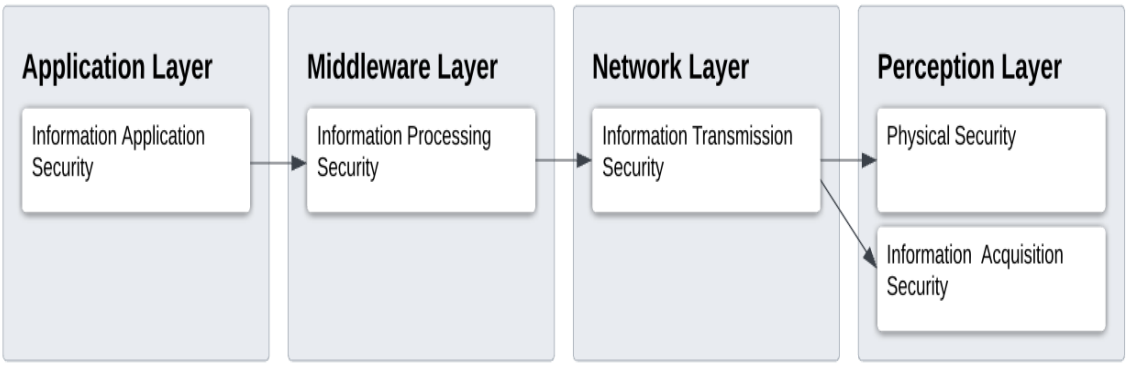


*Figure 8: Secured IoT architecture*

### 4.1.1. Perception Layer

The IoT's lowest layer is the perception layer. It is in charge of information collection across the whole IoT network. At the perception layer, physical security of hardware like RFID nodes, sensor devices, sensor terminals, and information generation and transmission security are the main concerns that should deal with. Physical security of IoT devices should be provided at the perception layer.

In the sensor network, architectures limitations can be listed such as DoS attacks, Physical control of sensor nodes and gateway nodes, eavesdropping, integrity and congestion attacks, and node duplication attacks. Unauthorized access, loss or destruction of personal information, duplication of SIM information, and impersonation of air interface information are some of the most serious security concerns surrounding sensor nodes in the internet of things (IoT). Security rules such as encryption methods, key distribution procedures, and intrusion detection systems must be used to provide a security architecture

for the sensor network [14]. Existing security frameworks include Tinysec and the LEAP protocol.

Symmetric and asymmetric key cryptography are the most common methods for protecting data. Because these measurements might be demanding for small portable devices, energy efficiency and compute power are limitations of these approaches. Biometric features, such as nerve interpulse intervals [4] or vascular blood volume [5], are used as alternative techniques of encrypting data transmitted between wearable sensing devices. Internal and external risks are the most common sorts of dangers to a smart home.

According to T. Xu et al. [53], hardware-based security is well-suited to meet IoT security needs. Due to its minimal space and energy needs, hardware-based security is a good starting point for the implementation of IoT protocols and processes. They provide elegant and effective solutions to a number of issues that traditional encryption has failed to address, such as safe location detection. It's critical to acknowledge that hardware-based security primitives and protocols have a number of severe drawbacks. Three stand out among them. The first is that their use was limited to secret key protocols until the introduction of the public physical unclonable function (PPUF). While the PPUF removes this constraint, the initial version of the PPUF imposed considerable time and energy overhead on at least one of the participants. The second is that owing to unavoidable device aging, the essential hardware-based security physical unclonable function (PUF) is quite unstable in terms of operating and environmental circumstances. The third disadvantage is that the earliest versions of PUFs use analog hardware, making integration into digital systems difficult or laborious.

Focus on safe multimedia authentication solutions for IoT data from wireless sensor networks in smart homes developed by Suryadevara et al. [24]. This paper showed authentication problems in data security could be brightened. Another authentication method, Secure Kerberos authentication is intended for IoT-based home automation systems [15]. In smart houses, a security mechanism of a terminal gateway group system is built, as well as a control system with numerous functions. Even if this approach solves the authentication problems, and works effectively, there are still incapability's for low processing power IoT devices.

### 4.1.2. Network Layer

In IoT-based smart home architecture, the primary task of the network layer is to transfer data over the network. Since IoT is based on a straightforward communication framework, Denial of Service (DoS) attacks, man-in-the-middle attacks, gateway attacks, storage attacks, etc. are the vulnerable point for this network. When data is transported via the network, the security strategy at the network layer must preserve authenticity, confidentiality, integrity, and data availability. Authentication, negotiation, intrusion detection and key management can be used to make the network resistant to such attacks [16].

New technologies, such as sensor networks, may be created to increase the safety of IoT networks (Li et al. [27]). Within a sensor network, important management techniques are successful. Establishing a temporary session key during communication can

improve secrecy, and authentication can be accomplished using non-symmetrical or symmetric cryptographic systems [27].

Winter, T. et al. [54] recommended the Routing Protocol (RPL) method for Low Power and Lossy Networks for IoT low power supplies. This recommended method is indefensible to various attacks because of the limited resource nature of IoT elements. Despite the fact that the RPL standard protects control communications with encryption, RPL is nevertheless vulnerable to internal attackers and selfish behavior.

Duan, X, et al.[55] presented a framework that analyzes the data vulnerability descriptions using machine learning and natural language processing before estimating vulnerability metrics. The expected metrics are then fed into a two-layer graphical security model. This model contains an attack tree in its first layer from the bottom to collect information specifically related to vulnerability problems from each node in the network, and the upper layer with an attack graph demonstrates the network connectivity. This security model automatically analyzes the security of the IoT network by collecting possible attack paths. From real-world IoT devices and probable vulnerabilities knowledge, a proof-of-concept intelligence structures type is used to evaluate the usefulness of its methods. The outcomes of the recommended framework indicate that new vulnerabilities can accurately predict vulnerability metrics with an average accuracy of over 90% and find the most vulnerable attack vectors within an IoT network. The assessment findings can be used as a reference for cybersecurity experts to take additional steps and minimize threats as soon as possible.

To address the security and privacy challenges of communication protocols in the IoT, Radomirovic [56] presents a dense IoT model as well as an adversarial model based

on the Dolev-Yao adversary. The opponent with corruption and fingerprinting skills has control of the communication network. The study highlights future efforts to develop a formal model that limits the adversary's capabilities.

M. Ge and D. S. Kim [57] present a methodology for assessing and modelling IoT security. The framework's major purpose is to show all conceivable attack vectors in the IoT, measure the efficiency of protection tactics using security metrics, and evaluate the security level of the IoT. i) Pre-processing, ii) security model improving, iii) storage and visualization, iv) security analysis and v) modifications and updates are the five processes in the framework. The writers discovered certain flaws in this framework's assessment part. They only use one vulnerability method, only analyse sensor networks with identical nodes, and assume the topology of the sample networks is static while assessing them.

### 4.1.3. Middleware Layer

In the IoT layered architecture, the middleware layer is responsible for processing data and providing an interface between the network and application layers. In the middleware layer, some of the existing technological challenges are linked to privacy, security, and dependability. The middleware layer is more secure when confidentiality and safe storage are guaranteed.

There are numerous middleware solutions supplied by technology firms, both open-source and commercial, that are all quite similar in terms of given capabilities, and no performance measurements or even rules to objectively assess this sort of software have been described in the literature.

The job of Middleware, according to Hammergren and Thomas [58], is analogous to that of a translator. Inside the network various devices use different communication methodologies, which is Different Application Programming Interfaces (APIs). Instead of learning every other API, the apps use middleware to connect with one another. Instead of learning how each program works, users edit data from one application, as shown in Figure 9. This allows users to concentrate on the topic at hand. At this point, the authors suggested that the middleware layer can be also used for security purposes. The data access middleware approach is one of the effective examples of this idea. Before translating data directly from the origin, it uses the authentication security protocol and access control protocols. Then it translates the data to a universal language. Because no one piece of middleware can be used in every situation, they are usually created for a specific set of circumstances.

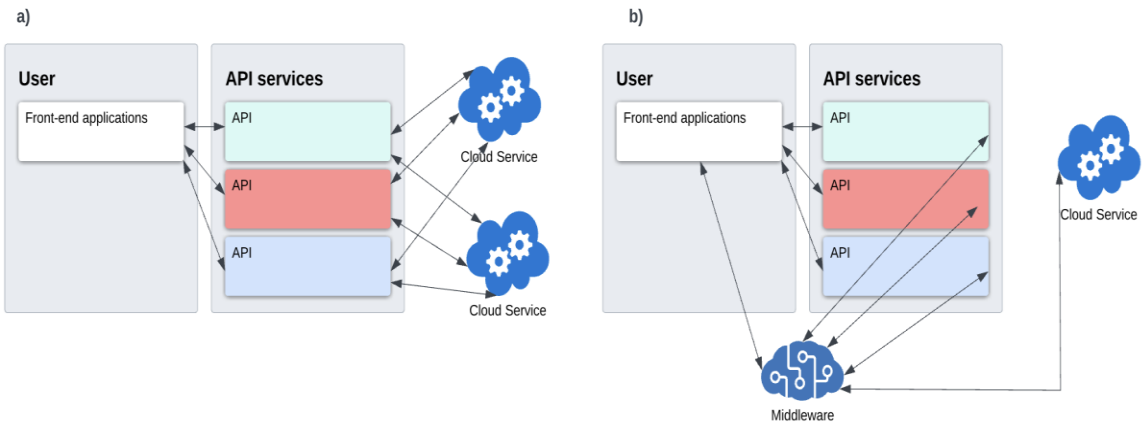


*Figure 9: Illustration of the communication (a) without middleware and (b) with middleware.*

### 4.1.4. Application Layer

Access controls must be controlled in order to prevent illegal access and use of data, which is a fundamental component of application layer security. The typical privacy protection technologies for maintaining database privacy may be based on data distortion technology and data encryption technology agents, to name a few. Data backup and recovery mechanisms must be correctly implemented in order to accomplish data security. TLS, SSL, DNS, and other data privacy mechanisms are examples.

Several studies on game-based security modeling for the IoT have been published since 2014. Their breadth, on the other hand, is limited to reducing the effects of certain threats [9] or emphasizing model solutions for specific domains [10], [11].

Chen et al. [9] recommended a fusion-based preservation mechanism in IoT systems to border the effects of intentional attacks. In this mechanism, authors explain the worst-case scenario. When the attacker has background knowledge related to the network topology and can reconcile all the nodes at once, they set up a zero-sum game between the defense plan and the attacker. Through the findings of performance evaluation, the suggested technique considerably improves the robustness of the IoT.

Kim and Lee [29] designed a recommendation system for managing IoT–network interactions between IoT devices, networks, and operation approaches aids in the implementation of appropriate schemes, the diagnosis of smart home data security issues, and the provision of advice on how to utilize household appliances. In smart homes, a hardware security module is required to improve appliance security and preserve data transmission efficiency across devices [4]. In smart home architectures, complex protection

systems are suggested for secure data transfer management and to avoid data loss in the course of data transfer inside the network. In order to deliver directions and forecasts in various scenarios, a recommendation system tailored exclusively for smart homes has been created. This is a pattern that occurs when a person uses two comparable devices at the same time, such as a music player and a DVD player. The recommendation system makes suggestions by looking at the patterns of the user's actions. Bhole et al. [11] used the recommendation system architecture for data security purposes in their proposed solution. Because recommendations systems are learning from specific user behaviors, this method couldn’t be helpful for security purposes [9].

Mainetti et al. [28] described a software ecosystem that has been devised and built that allows users with various expertise to construct location-aware applications for autonomously managing smart homes. For the communication mechanism between the embedded devices hardware and software solutions are employed in the beginning state of the implementation. Bluetooth is employed to measure the distance more accurately between IoT devices and mobile devices.

As a result, security measures on cloud gateways are required to prevent malicious actors from altering settings. At the application layer, biometrics and multi-level authentication might be a useful option for access control.

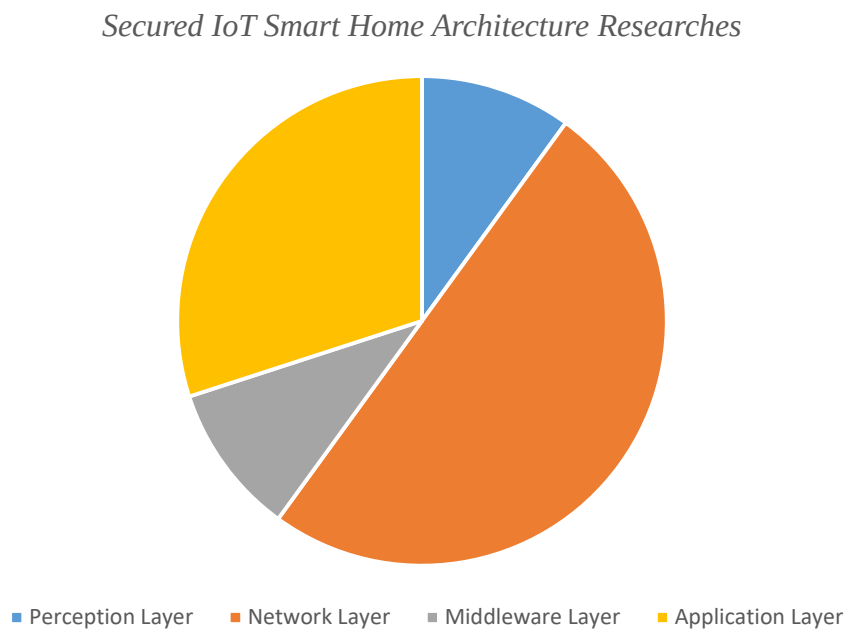


*Figure 10: Distribution of Researches in the Secured IoT Smart Home Architecture*

*Table 4: Existing methods providing security and their limitations*

| Layer/ Method/Author | Issues it addresses | Solutions | Limitations |
|---|---|---|---|
| Perception Layer/ Hardware-based security (PPUF, PUF)/ T. Xu et al [53] | Number of issues that traditional encryption | Provide elegant and effective solutions to traditional encryption | Restricted to secret key protocols<br>Unstable due to unavoidable device aging<br>The first generations of PUFs are analog circuitry |
| Network Layer/ Sensor networks/ Li et al. [27] | Safety of sensor networks | Establishing a temporary session key, using non-symmetrical or symmetric cryptographic systems | Slow working time<br>Restricted to secret key protocols |
| Network Layer/ RPL/ Winter, T. et al. [54] | Low processing power | Routing Protocol for Low-power and Lossy Networks | Vulnerable to internal attackers and selfish behavior |
| Network Layer ML and NLP Framework/ Duan, X, et al.[55] | Vulnerabilities in the IoT smart home networks | Analyzes vulnerability descriptions using machine learning and natural language processing | Results are so good but still have issues related to complex process in the framework. |
| Network Layer/ Dense IoT model/ Radomirovic [56] | Security and privacy challenges of communication protocols | Highlights future efforts to develop a formal model that limits the adversary's capabilities | This method only proposed |
| Network Layer/ Modeling IoT security/ M. Ge and D. S. Kim [57] | Show all conceivable attack vectors in the IoT | Efficiency of protection tactics using security metrics, and evaluate the security level of the IoT | Considering Different Defense Strategies<br>Addressing the Heterogeneity<br>Tackling the Mobility |
| Middleware Layer/ New Middleware methods/ Hammergren and Thomas [58] | Heterogeneity of IoT program works | Users edit data from one application | Usually created for a specific set of circumstances |
| Application Layer/ Fusion-based protection mechanism/ Chen et al. [9] | Attacker knows the network architecture | To limit the effects of purposeful assaults using zero-sum game | The findings of performance evaluation, the suggested technique considerably improves the robustness of the IoT |
| Application Layer/ Designed a recommendation system/ Kim and Lee [29] | Data loss during data transmission inside a network | Aids in the implementation of appropriate schemes, the diagnosis of smart home data security issues | Recommendations systems are learning from specific user behaviors, this method couldn't be helpful for security purposes |
| Application Layer/ Software ecosystem/ Mainetti et al.[28] | Communication mechanisms between IoT smart home devices | Bluetooth protocols are the main component of this method | Bluetooth technology is not suitable for long distance communications |

In the Pang et al. [39] proposed architecture three parts are used to create a simple smart home system: a home gateway, a cloud server, and a user interface. It looks similar to traditional smart home architecture but they used an advanced intrusion firewall for their home gateway. Devices with machine-to-machine integration are conceived and deployed for smart home systems. Hu et al. [35] use a similar approach with small differences. Smart house gateways for the social Web of Things are planned and deployed using IoT-based media content sharing services in home automation in his method. Wei and Qin [44] focus on the economic perfective of effective solutions. Under IoT systems and cloud computing, a system and application of low-cost smart houses are built.

Pereni and Krajovi [34] presented a smart house design, home automation management system, and HLSM (Home Localization System for Misplaced Objects). HLSM, in particular, entails connecting several devices to a central server through Ethernet or Wi-Fi, depending on the reader type. The mobile readers then use Wi-Fi to interact with the server. This technology aids in the discovery of items such as glasses, wallets, and keys in IoT-enabled smart homes. This approach is ideal for applications with a short range. Even though this technology makes use of Wi-Fi technologies, it has significant limitations in terms of long-range applications. It also contains the central server smart home drawbacks.

Another data security-related research area is energy-consuming. IoT devices are able to understand and decide the usage of energy in smart homes. Home automation with wireless power control and an energy management system is aimed to minimize energy usage in smart households [16]. When users discover energy waste, a system is created to

make advice. To reduce energy waste in smart homes, a ZigBee wireless device was devised and installed by Fernández-Caramés [29]. Sockets are created with sophisticated control and energy management in mind. A system based on IoT home and ZigBee/GPS technologies has been created and implemented. In smart homes, ZigBee devices are being developed and installed. Application systems and their architectures assist the smart home future developments and applications which are designed for IoT devices. Zhang et al. [45], General Packet Radio Service (GPRS), and ZigBee-based smart home control systems have been created. To regulate power usage, another ZigBee-based system was created and installed by Yongqing and Dan [40]. ZigBee-based systems are suitable for the smart home. ZigBee is specifically designed for IoT devices.

As a security framework architecture, BlinkToSCoAP is being developed as an IoT data security management framework for IoT devices in smart homes (Peretti et al. [31]). This framework is specifically developed for cloud-based smart homes. This framework was created in order to provide a completely secure smart home automation system. To accomplish network virtualization in smart homes, a middleware framework for sensor nodes is being developed. In addition to that, it includes high level authentication and access control protocols for providing the data integrity and confidentiality. Because of limitations on the IoT devices' capacity, this approach couldn't become a standard protocol [15].

Li et al. [27] developed a broad framework to address the security needs of a cloud–IoT paradigm, which they then applied to remote mobile monitoring. A smart home controller application communication structure is presented in depth. Data transfer becomes more secure in this manner. In smart homes, a framework for exchanging data

with numerous technologies is being created. The goal of a created framework is to provide a full software tool chain to address the data loss because of the IoT integration difficulties in smart homes in general.

There are two forms of new technologies that have recently piqued people's curiosity. Popular emerging technologies that intersect with IoT security solutions include SDN (software defined network) and blockchain.

The primary concept of SDN is to decouple network and data control. In order to cope with difficulties in the IoT environment, such as resource allocation in IoT devices, both centralized control and dynamic network management are possible. Furthermore, several existing IoT concerns, such as dependability, security, scalability, and quality of service (QoS), may be effectively solved. Although device links are useful for defect diagnosis and semantic suggestions in smart home systems, creating these associations is difficult for consumers. As a result, an automated generating strategy is proposed to relieve customers and service providers of the load. An SDN-based home cloud detects device information such as model name, manufacturer, and network protocol when an IoT device connects to a home switch. The packets that transit via SDN switches are simply captured by the SDN controller. As a result, the controller generates a status graph with information for each IoT device. It automatically builds four social ties based on the information after detecting the IoT device. To offer a semantic inquiry, the status is kept in RDF/XML format.

Blockchain technologies receive a lot of success in financial applications. Currently, the Blockchain technologies are stable and working effectively. Now it is ready to use in other sectors' applications. IoT is one of them. Secure and private transactions, as

well as decentralization of communications and procedures, will benefit IoT-based applications [31]. The benefits of blockchain technology for the IoT include decentralization, pseudonymity, and safe transactions.

# 5. DISCUSSION AND LESSONS LEARNED

The security of smart house designs based on IoT applications is a critical issue for general smart home occupants, and research is needed to give a better solution for patient security, privacy protection, and the security of users' entities from being stolen or compromised. Innovative technology has a variety of restrictions in this area. To give important perspectives for technological settings and researchers, the present gaps and trends in this field should be examined. The following sections present and offer the recognized basic features of this growing area. To be completely embraced in smart house applications, open issues encountered in the development of IoT-based smart home security are solved.

Table 5 presents the number of articles that have been gathered from the literature. In terms of the paper's categorizations, we divided our final research paper dataset into three subtopics. Papers related to developing and/or designing a new method or approach for security problems. The next topic focuses on the review and survey papers. The last group includes the evaluation or comparison of the methods and/or approaches. The articles were compiled based on their sources, namely, Scopus, Science, Direct, and IEEE Explore, which are considered the most reliable sources of scientific research. A total of 58 articles from these sources. All of these studies have focused on the access to smart homes environment's internet of things devices to assist users and individuals lead a decent life.

*Table 5: The number of articles that have been gathered from the literature*

| Topic | Smart Home Security | Number of Papers |
|---|---|---|
| Develop & Design | Device Security | 4 |
| | Network Security | 10 |
| | Cloud Security | 8 |
| | Application Security | 13 |
| Review & Survey | Device Security | 2 |
| | Network Security | 7 |
| | Cloud Security | 4 |
| | Application Security | 6 |
| Evaluation & Comparative | Device Security | 1 |
| | Network Security | 5 |
| | Cloud Security | 3 |
| | Application Security | 11 |

The thesis goal is to look at existing research, especially using tools, that considers the safety concerns caused by security flaws in IoT apps. Different areas of comparison are taken into consideration, such as analytic methodologies, safety and security requirements formulation and verification in IoT apps, how to express these requirements, and the interacting environment. As a result, we can shed light on the major flaws and issues in the examination of IoT Apps' safety and security. We've recently seen a surge in new IoT platforms, which poses a new challenge: how to manage heterogeneous IoT systems in a single operating environment. This is a topic that can be explored further. Some of the literature tools may be enhanced so that the analysis process could be carried out in a single environment with multiple IoT apps from different IoT platforms. The research into Denial-of-Service (DoS) assaults that may occur in IoT networks, as well as a robust model that can swiftly identify and neutralize such attacks, is still in its early stages. IoT devices

are often connected to an unstable network using protocols such as 6LoWPAN and IPv6. Despite the devices' strong encryption and authentication mechanisms, they may be vulnerable to assaults from both inside and outside the network. An intrusion detection approach might be effective in combating these attempts. The study also provides insight into future research directions that will be required to close the gaps.

According to our research, there aren't many intrusion detection systems for IPv6-connected IoT devices. Existing IDS solutions are mostly for WSNs or the conventional Internet.

Overall, we discovered security flaws in IoT design, lightweight security solutions, and managing large amounts of heterogeneous data as a result of our research. Application-specific security needs exist for IoT. However, we may provide a common framework that can be adjusted to meet the needs of the application. We may use software engineering ideas to highlight the commonalities between IoT apps and develop a common framework that can offer these applications with the appropriate security solutions.

Due to the limited resource construction of IoT, lightweight security solutions are an important subject of future work. As a result, lightweight security issues are an important factor to consider before installing sophisticated IoT devices. Key management, authentication, authorization, access control, and other security systems should be energy efficient and lightweight. We can finally provide a universal IoT security system. Authentication and encryption may be viable options for addressing IoT security concerns. However, implementation of effective authentication and encryption for low-power, computationally and resource limited devices is still in its infancy and does not ensure the prohibition of hostile nodes in the network, such as damaged devices or PCs. AAA

(authentication, authorization, accounting), EAP (extensible authentication protocol), and CoAP are used in a demanding setting such as a smart city.

Combining formal approaches with machine learning to discover probable security flaws in various levels of IoT systems is another interesting research path to consider. A thorough mathematical and logical assurance for the safety and security properties of an IoT application may be provided using the formal approach. To better the study of IoT systems, certain literature tools explore using various Artificial Intelligence (AI) and Machine Learning (ML) approaches. Though the methodology has a number of drawbacks (for example, state space explosion, high maintenance costs, and a steep learning curve), recent formal methods work has advanced to the point where it may be used to solve security concerns both during development and at run-time. In addition, both professionals and academics are increasingly using machine learning for different parts of IoT, and they may be utilized in conjunction with formal approaches to give rigorous yet scalable security guarantees for mission-critical IoT systems.

Every second, an IoT system generates a massive volume of heterogeneous data. In the future, we will focus our research on the most effective way to manage the massive amounts of data created by IoT systems. For enormous data interchange in a network, we may use technologies like big data, blockchain, cloud, and fog computing. The technologies are capable of safely and efficiently managing heterogeneous large amounts of data. To achieve complete security solutions for the applications, it would be a good idea to employ big data, cloud, and fog computing technologies to IoT systems.

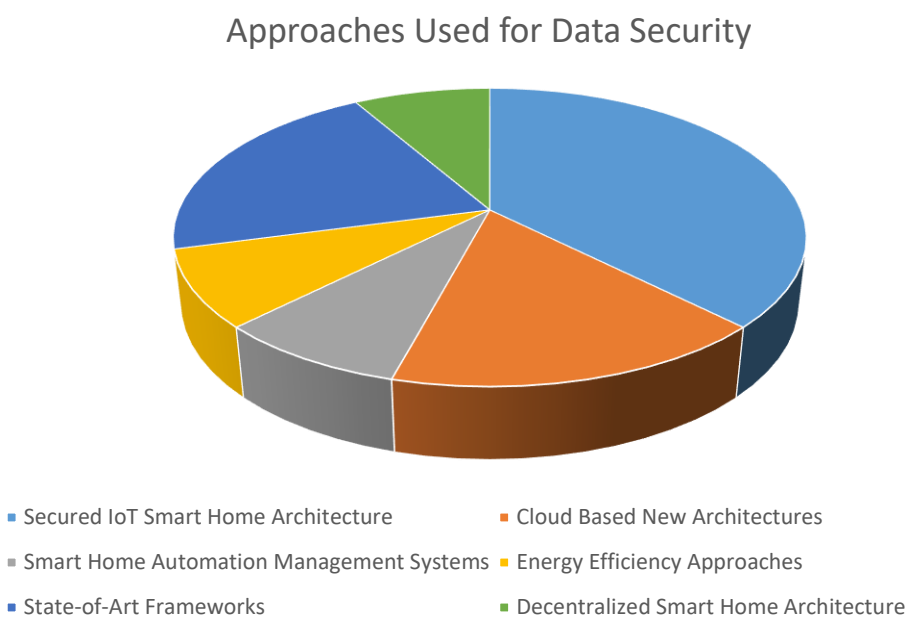


*Figure 11: Distribution of Researches on Approaches Used for Data Security*

When undertaking the analytical process, certain literature techniques do not consider formalizing Security and Safety features to be fully automated. We discovered that many of the literature tools focused on assessing the IoT system by knowing its components, rather than infusing the system with Security and Safety features. For security and safety properties, some technologies employ a text-based description and do manual compliance to IoT system analysis toward these properties. Other tools have addressed this issue, however their analysis method relied on translating the IoT system into many representations, which has an impact on the overall analysis performance. This procedure is particularly complicated by the lack of security and safety regulations in IoT devices.

The importance of maintaining privacy in this scenario cannot be overstated. Research must conduct future search on security for privacy while keeping in mind the features and security requirements of IoT. In order to provide a lightweight security

solution, bitwise operations [10] rather than mathematical algorithms like ECC (elliptic curve cryptography) must be used for encryption and authentication. Dynamic prevention, detection, diagnosis, and isolation can all be supported by embedded security [7]. Furthermore, manufacturers frequently use hardcoded credentials or passwords for convenience, which usually results in a substantial authentication failure.

# 6. CONCLUSION

Owing to the Internet of Things, people can work and live more intelligently and have more management over their daily lives. The crucial topic of making smart home systems more automatic, working independently is provided by the IoT devices. The Internet of Things is one of the most significant improvements in recent years for people's daily lives and will continue to earn traction as more organizations see the importance of connected devices in staying competitive. Cyber security, both for the wireless and wired elements of the systems, is one of the most serious concerns of the emerging requirements confronting smart grid development. Through the network connections, IoT devices are able to send and receive a big amount of data every time. This allowed the attackers to get access to the IoT networks and steal their valuable data. Cyber terrorists might target the smart grid, which is a serious worry for system designers.

The primary goal of IoT security is to protect users' privacy and confidentiality, secure the security of IoT infrastructures, data, and devices, and assure the availability of IoT ecosystem services. Consequently, IoT data safety and security research has admitted lots of attention lately, with the help of reachable computing and analysis platforms, modelers, and simulation tools.

The potential and intelligence of IoT devices, as well as their exploitation, are both wide open. Because there is a lack of standards in the IoT sector, every single connection

may put the network at risk. A uniform IoT architecture is still a work in progress. The security and privacy risks in the IoT realm were emphasized in this article. IoT security is divided into multiple layers of abstraction and dimensions. The degrees of abstraction span from physical layers of sensors, processing and communication, and devices to the semantic layer, which interprets and processes all acquired data. Because software is now the most popular and can simultaneously cover a huge number of devices and processes, it is expected that the bulk of security assaults will occur at the software level. The majority of innovative attacks in terms of research are on the network layer, namely semantic assaults during data processing and decision-making phases. Because of the way data is exchanged, the Internet of Things is inherently vulnerable to the majority of wireless network assaults. As a result, IoT requires a security strategy, but it must be provided at the lowest feasible cost. In order to offer authenticity, integrity, and secrecy, several ways that give security lightweight crypto-primitives should be researched [11], [18].

This thesis makes a significant addition by conducting a detailed survey and categorization of publications on the subject. There are certain distinct patterns in the literature that have been identified. The current research on smart homes, IoT security, data security, and privacy on IoT devices was covered in the literature study. Several articles provide an overview of the issue, while others look at existing smart home applications. Some research projects result in real-world applications for smart houses. We guided a comprehensive review of the literature to identify issues, benefits, and recommendations for IoT-enabled smart homes. The findings reveal certain inconsistencies in the utilization of communication components in smart home technology. Several suggestions for managing and regulating these components are made in this regard.

Researchers are interested in IoT security. As a result, this study compiled a list of typical security issues and recommended security solutions for them in the context of data security in smart homes. Then we compared these research-based recommended solution schemas. While comparing, we consider factors such as how powerful the method is, how successful it is at solving issues, and if it is suited for universal use across all IoT devices. Then we go over the benefits and drawbacks of current data security solutions for smart homes.

To decrease their power consumption, provide safe and secure conditions, accomplish proper and dependable administration of different control devices, and improve their user experience, users must follow the instructions on how to use these components. In addition, the thesis explored the key issues in protecting IoT and the security services needed in IoT. We've also included a quick summary of existing techniques to safeguarding IoT platforms. The most controversial topic in the literature is there is no common compromise on how to develop security on the limited resources of IoT devices. Traditional IoT network protocols and security methods need be improved to meet the technology's security requirements. The issue with IoT devices is that they have a low-performance CPU, limited memory, and low-power batteries. Existing security solutions used in computer networks are challenging to deploy in IoT devices because of these components. In the IoT, a suite of lightweight algorithms to block various forms of threats is required.

Another finding from the literature review is that there is still a point to generate or a recommendation for building a standard protocol to address IoT security issues. In other

words, no clear, standardized manner of characterizing the state of cybersecurity readiness in terms of IoT device security has been discovered. All security systems should provide integrity, confidentiality, and non-repudiation at the same time inside the systems. The IEEE (Institute of Electrical and Electronics Engineers) and IETF (Internet Engineering Task Force) focus mainly on security and communication protocols problems for IoT and internet connectivity.

The myriad problems related to the use of Internet of things devices in smart homes are addressed. Also, the recommendation to solve or improve the security of those problems are explained. Future research will be able to implement those solutions. The majority of these issues are on safety, security, energy usage, and control. The concepts given in the associated literature are also summarized in this review, making it a useful resource for scholars.

## REFERENCES


1. A. F. A. Rahman, M. Daud, M. Z. Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework", *ICC (International Conference on Internet of things and Cloud Computing),* United Kingdom, Article No.: 79, March 2016

2. Ahmed, M., Sharif, L. Kabir, M. Al-Maimani, M, "Human Errors in Information Security," International Journal, 1(3), 2012.

3. Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on Internet of Things. Journal of Network and Computer Applications, 97, 48-65.

4. Hejazi, H., Rajab, H., Cinkler, T., & Lengyel, L. (2018, January). Survey of platforms for massive IoT. In *2018 IEEE International Conference on Future IoT Technologies (Future IoT)* (pp. 1-8). IEEE.

5. Amadeo, M., Campolo, C., Iera, A., & Molinaro, A. (2015, June). Information Centric Networking in IoT scenarios: The case of a smart home. *In 2015 IEEE international conference on communications (ICC) (pp. 648-653)*. IEEE.

6. *Global IOT market size grew 22% in 2021- these 16 factors affect the growth trajectory to 2027.* IoT Analytics. (2022, March 30). Retrieved March 31, 2022, from https://iot-analytics.com/iot-market-size/

7. Arunvivek, J., Srinath, S., & Balamurugan, M. S. (2015). Framework development in home automation to provide control and security for home automated devices. *Indian Journal of Science and Technology*, 8(19).

8. Bhide, V. H., & Wagh, S. (2015, April). i-learning IoT: An intelligent self-learning system for home automation using IoT. *In 2015 international conference on communications and signal processing (iccsp) (pp. 1763-1767).* IEEE.

9. Bian, J., Fan, D., & Zhang, J. (2011, October). The new intelligent home control system based on the dynamic and intelligent gateway. *In 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology (pp. 526-530).* IEEE.

10. Bourobou, S. T. M., & Yoo, Y. (2015). User activity recognition in smart homes using pattern clustering applied to temporal ANN algorithm. Sensors, 15(5), 11953-11971.

11. Cebrat, G. (2014, May). Secure web based home automation: Application layer based security using embedded programmable logic controller. *In 2014 2nd International Conference on Information and Communication Technology (ICoICT)* (pp. 302-307). IEEE.

12. Chan, M, Estève, D, Escriba, C, Campo, E. A review of smart homes – present state and future challenges. Comput Meth Prog Biomed 2008; 91(1): 55–81.

13. Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, *63*, 363-374.

14. Cho, H., Ji, J., Chen, Z., Park, H., & Lee, W. (2015). Measuring a distance between things with improved accuracy. Procedia Computer Science, 52, 1083-1088.

15. Cong, YP, Wei, ZQ, Hu, MD. A Smart Home architecture based on concept ontology. Appl Mech Mater 2013; 303–306(February): 1559–1564.

16. Datta, S. K. (2016, January). Towards securing discovery services in Internet of Things. *In 2016 IEEE International Conference on Consumer Electronics (ICCE) (pp. 506-507).* IEEE.

17. CCMB-2017-04-001. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model Ver. 3.1, Rev. 5, The Common

Criteria. April 2017; p. 2. Available online: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed on 15 September 2021).

18. ISASecure. IEC 62443—EDSA Certification. Available online: https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification (accessed on 15 September 2021).

19. de Oliveira, G., Oliveira, O.d.F., de Abreu, S. *et al.* Opportunities and accessibility challenges for open-source general-purpose home automation mobile applications for visually disabled users. *Multimed Tools Appl* (2022). https://doi.org/10.1007/s11042-022-12074-0.

20. Framework for Improving Critical Infrastructure Cybersecurity v1.1; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, April 2018.

21. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Commun. Surv. Tutor*. 2015, 17, 1294–1312.

22. Greensmith, J. (2015, July). Securing the internet of things with responsive artificial immune systems. *In Proceedings of the 2015 annual conference on genetic and evolutionary computation (pp. 113-120).*

23. Han, J. H., Jeon, Y., & Kim, J. (2015, October). Security considerations for secure and trustworthy smart home system in the IoT environment. *In 2015 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 1116-1118). IEEE.

24. Hasibuan, A., Mustadi, M., Syamsuddin, I. E. Y., & Rosidi, I. M. A. (2015, November). Design and implementation of modular home automation based on wireless network, REST API, and WebSocket. *In 2015 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)* (pp. 362-367). IEEE.

25. Harper, R Inside the Smart Home: ideas, possibilities and methods. In: Harper, R (eds). *Inside the Smart Home, London, UK*: Springer, 2013, pp. 1–13.

26. Devalal, S., & Karthikeyan, A. (2018, March). LoRa technology-an overview. In *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 284-290). IEEE.

27. Li, F., et al., 2012. Research on sensor-gateway-terminal security mechanism of smart home based on IOT. (Ed.), *Internet of Things, Communications in Computer and Information Science*, Springer, Berlin, Heidelberg, vol. 312, pp. 415–422.

28. ISO/IEC DIS 27400. Cybersecurity: IoT Security and Privacy—Guidelines; ISO: Geneva, Switzerland, 2021; Available online:https://www.iso.org/standard/44373.html (accessed on 13 December 2021)

29. Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems*, 56, 719-733.

30. Jiang, Y., Liu, X., & Lian, S. (2016). Design and implementation of smart-home monitoring system with the internet of things technology. *In Wireless Communications, Networking and Applications (pp. 473-484).* Springer, New Delhi.

31. Tchagna Kouanou, A., Tchito Tchapga, C., Sone Ekonde, M., Monthe, V., Mezatio, B. A., Manga, J., ... & Muhozam, Y. (2022). Securing Data in an Internet of Things Network Using Blockchain Technology: Smart Home Case. *SN Computer Science*, 3(2), 1-10.

32. ISO/IEC 30141. Internet of Things (loT)—Reference Architecture; ISO: Geneva, Switzerland, 2018; Available online: https://www.iso.org/standard/65695.html (accessed on 18 October 2021).

33. Basili, V.; Caldiera, C.; Rombach, D. Goal, question, metric paradigm. In *Encyclopedia of Software Engineering*; Wiley: Hoboken, NJ, USA, 1994; Volume 2, pp. 527–532. ISBN 1-54004-8. Available online: http://www.kiv.zcu.cz/~{}brada/files/aswi/cteni/basili92goal-question-metric.pdf (accessed on 15 September 2021).

34. Kailas, A, Cecchi, V, Mukherjee, A A survey of contemporary technologies for Smart Home energy management. *In: Obaidat, MS (eds). Handbook of green information and communication systems*, Waltham, USA: Elsevier, 2012, pp. 35–56.

35. Khalid, Z., Fisal, N., Rozaini, M., Safdar, H., Ullah, R., & Maqbool, W. (2014, April). Middleware framework for network virtualization in SHAAL. *In 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)* (pp. 175-179). IEEE.

36. Kirkham, T., Armstrong, D., Djemame, K., & Jiang, M. (2014). Risk driven Smart Home resource management using cloud services. *Future Generation Computer Systems*, 38, 13-22.

37. Lee, Y. T., Hsiao, W. H., Huang, C. M., & Seng-cho, T. C. (2016). An integrated cloud-based smart home management system with community hierarchy. IEEE Transactions on Consumer Electronics, 62(1), 1-9.

38. Li, B., & Yu, J. (2011). Research and application on the smart home based on component technologies and Internet of Things. Procedia Engineering, 15, 2087-2092.

39. Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J., & Tenhunen, H. (2015). SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, 52, 452-459.

40. M.R. Alam, M.B.I. Reaz and M.A.M. Ali, 2011. Statistical Modeling of the Resident's Activity Interval in Smart Homes. *Journal of Applied Sciences*, 11: 3058-3061.

41. Perešíni, O., & Krajčovič, T. (2015, September). Internet controlled embedded system for intelligent sensors and actuators operation. *In 2015 International Conference on Applied Electronics (AE) (pp. 185-188).* IEEE.

42. Sezer, O. B., Can, S. Z., & Dogdu, E. (2015, June). Development of a smart home ontology and the implementation of a semantic sensor network simulator: An Internet of Things approach. *In 2015 International Conference on Collaboration Technologies and Systems (CTS)* (pp. 12-18). IEEE.

43. Solaimani, S., Keijzer-Broers, W., & Bouwman, H. (2015). What we do – and don't – know about the Smart Home: An analysis of the Smart Home literature. Indoor and Built Environment, 24(3), 370–383. https://doi.org/10.1177/1420326X13516350

44. T. Kramp, R. van Kranenburg, S. Lange, Introduction to the Internet of Things, *in: Enabling Things to Talk,* Springer, Berlin, Heidelberg, 2013, pp. 1–10, doi: 10.1007/978- 3- 642- 40403- 0 _ 1.

45. Thiyagarajan, M., & Raveendra, C. (2015, October). Integration in the physical world in IoT using android mobile application. *In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 790-795). IEEE.

46. Ye, X., & Huang, J. (2011, December). A framework for cloud-based smart home. *In Proceedings of 2011 international conference on computer science and network technology (Vol. 2, pp. 894-897).* IEEE.

47. Zhang, W., Li, G., & Gao, W. (2015). The embedded smart home control system based on GPRS and Zigbee. *In MATEC Web of Conferences (Vol. 34, p. 04010).* EDP Sciences.

48. Z.K. Zhang, M. C. Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh, "IoT security: ongoing challenges and research opportunities", *Service-Oriented Computing and Applications (SOCA),* Matsue, Japan, pp. 230-234, November 2014

49. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. *In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST),* London, UK, 14–16 December 2015.

50. Krebs, B. *Who Makes the IoT Things Under Attack? Krebs on Security*, Oct. 3, 2016, Virginia, USA. Available online: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/ (accessed on 15 September 2021)

51. B. V. S. Krishna and T. Gnanasekaran, "A systematic study of security issues in Internet-of-Things (IoT)," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017*, pp. 107-111, doi: 10.1109/I-SMAC.2017.8058318.

52. Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of cleaner production, 140*, 1454-1464.

53. T. Xu, J. B. Wendt and M. Potkonjak, "Security of IoT systems: Design challenges and opportunities," *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014, pp. 417-423, doi: 10.1109/ICCAD.2014.7001385.

54. Winter, T., Thubert, P., Brandt, A., Hui, J. W., Kelsey, R., Levis, P., ... & Alexander, R. K. (2012). RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. *rfc*, 6550, 1-157.

55. Duan, X., Ge, M., Le, T. H. M., Ullah, F., Gao, S., Lu, X., & Babar, M. A. (2021, December). Automated Security Assessment for the Internet of Things. In *2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC)* (pp. 47-56). IEEE.

56. S. Radomirovic, "Towards a Model for Security and Privacy in the Internet of Things", *Proceedings of 1st International Workshop Security of the Internet of Things (SecloT 2010). 2010*

57. M. Ge and D. S. Kim, "A Framework for Modeling and Assessing Security of the Internet of Things," *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)*, 2015, pp. 776-781, doi: 10.1109/ICPADS.2015.102

58. Hammergren, T. C. (2009). *Data Warehousing for dummies.* John Wiley & Sons.