The Journal of Supercomputing (2021) 77:14053–14089
https://doi.org/10.1007/s11227-021-03825-1

Smart home security: challenges, issues and solutions at different IoT layers

Haseeb Touqeer[1] · Shakir Zaman[1] · Rashid Amin[1] · Mudassar Hussain[2] · Fadi Al-Turjman[3] · Muhammad Bilal[4]

Accepted: 17 April 2021 / Published online: 10 May 2021

Abstract
The Internet of Things is a rapidly evolving technology in which interconnected computing devices and sensors share data over the network to decipher different problems and deliver new services. For example, IoT is the key enabling technology for smart homes. Smart home technology provides many facilities to users like temperature monitoring, smoke detection, automatic light control, smart locks, etc. However, it also opens the door to new set of security and privacy issues, for example, the private data of users can be accessed by taking control over surveillance devices or activating false fire alarms, etc. These challenges make smart homes feeble to various types of security attacks and people are reluctant to adopt this technology due to the security issues. In this survey paper, we throw light on IoT, how IoT is growing, objects and their specifications, the layered structure of the IoT environment, and various security challenges for each layer that occur in the smart home. This paper not only presents the challenges and issues that emerge in IoT-based smart homes but also presents some solutions that would help to overcome these security challenges.

Keywords Smart cities · Smart home · Security · IoT · Protocols

1 Introduction

With the beginning of the twenty-first century, the world has entered the Internet era; the way people live and work has changed. Due to rapid development in the world of information and the Internet, another application of the Internet came into

✉ Rashid Amin
rashid4nw@gmail.com

✉ Muhammad Bilal
m.bilal@ieee.org

Extended author information available on the last page of the article

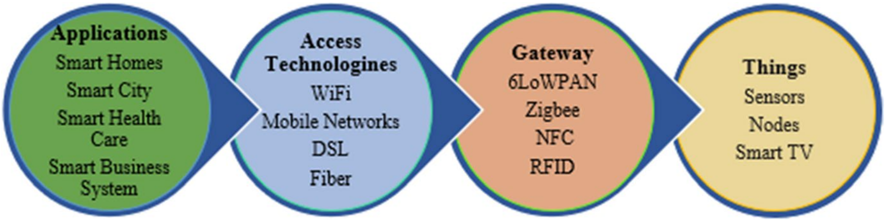
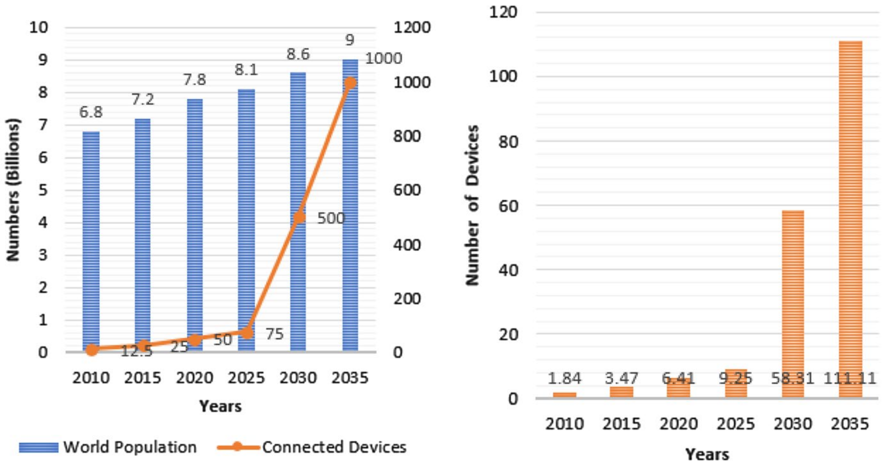


Fig. 1 Major component of IoT structure and its applications

existence, known as the Internet of Things (IoT). IoT is a ubiquitous network in which devices communicate with no human interaction. It follows the mechanism in which the physical environment is controlled by analyzing and processing the data generated by sensor devices [76]. Sensors play an important role in the IoT environment as the data is perceived or collected by these sensors and then sent to the central body for further process [93]. Over the past few decades, the microprocessor controller is being used in different devices. IoT augments one more module to these devices, that is Internet connectivity. Smart devices like smart televisions, smart mobiles, smart doors, and smart heaters get connected through the Internet with each other to provide information, hence providing comfort to humans [119]. Figure 1 shows the applications and formation of the IoT environment.

A survey by Cisco revealed that in 2010 Internet-connected devices were 12.5 billion. In 2015, it reached 25 billion; in 2020, it reached 50 billion; in 2025, 75 billion; in 2030, it will touch 500 billion [34], and by the end of 2035, it will reach till 1 trillion. According to another survey done by the International Data Corporation, it is predicted that over 200 million devices will have a network connection by 2020. United Nations population fund states that the world population will reach 8.1 billion by 2025, and according to the United Nations Department of Economic and social affairs by 2030 population will reach 8.6 billion. It will reach 9 billion by the end of 2035. Figure 2 shows the world population, active connected devices on the Internet, and an average number of devices own by a single person in graphical representation.

A smart home is an application of IoT environment, which comprises of physical components and Internet connectivity. These devices communicate with each other and provide innovative and smart services to the user [1, 96]. Smart heaters, smart coolers, smart televisions, smart watches, mobile devices, and smart locks are IoT-based smart home appliances that are connected with the Internet and make the life of a human more comfortable [2, 74]. With a smart home automation environment, we can control and monitor the home appliances, such as lighting, temperature, the climate of home, doors, and windows [44]. Although smart homes are more convenient to use and control all home appliances, however, due to the Internet connectivity as well as the dynamic and heterogeneous nature, the smart homes are facing different security issues [125]. As in smart homes environment, plethora of smart devices are interconnected and require information exchange, the architecture of IoT environment has become heterogeneous and due to the heterogeneity, these devices



(a) World population and connected devices

(b) Average no. of connected devices per person

Fig. 2 World population, active devices and average no. of connected devices per person

are vulnerable to security attacks [64]. ISO 27005 defined attack as the ability to take over the vulnerabilities of the premises and lead the organization to a huge loss [54]. Security attack in the digital world is termed as an illegal activity performed by an intruder against a network and get access to the network to make changes that can lead users to the loss of their sensitive data [82]. An attacker can monitor the different activities of the smart home user through the information collected by the smart devices [77]. Furthermore, an intruder may take control of the smart home devices remotely and can use the devices for his malicious purposes, causing billion dollars lost to the owner of a smart home. Successful attacks on various commercial off-the-shelf products have been performed.

These attacks are not only hypothetical, e.g., in 2014, over 73,000 video cameras were also found to be streaming their surveillance footage on the web. As discussed in [4], in 2016, every IoT device was attacked once in every two minutes. According to a recent study by H.P., currently, almost 70% of smart devices are vulnerable to security threats. Another study by H.P. reveals that 90% of devices have collected personal information during the testing phase. This data can be used for malicious purposes due to a compromised device or as a result of a cyber-attack. Hence, the user will be reluctant to use these smart devices due to their vulnerability to security attacks [60]. The proposed work gives a revelation about the security issues in Smart Homes. This work comprises the security issues at the IoT's layer and discusses the solutions to those problems. In today's life, where the Internet is overwhelmed, it causes numerous security issues. Thus it is needed to educate people about malicious activities over the Internet. This survey aims to alert users before using IoT services in their daily lives. In this way, they have adequate knowledge about the breaches and thus can save themselves from concealed attacks.

Among several issues, wireless network security is the highest priority issue to be solved for the IoT. There are numerous surveys in the literature for IoT's issues and solutions, however, not all existing surveys cover all the issues and related solutions. They generally cover partially each IoT layer regarding security challenges and related countermeasures. Finding each issue and solution for that issue is the motivation behind this survey over IoT, security issues, and solutions at each layer. In this paper, we present an overview of IoT architecture and layer assembly of the IoT network environment. We also elaborate a systematic study of the critical security problems and mitigation approaches. The contributions of this survey paper are as follows:

1. We discuss the IoT growth, working of IoT, and frequency of attacks in the past.
2. We elaborate IoT in the form of four-layer architecture.
3. We identify security challenges faced by the IoT environment at each IoT network layer.
4. We suggest a mitigation strategy to almost each security issue.

The discussion proceeds with related work in Sect. 2. Section 3 elaborates on IoT, how IoT works, its applications, IoT layers structure, and also various security problems. Section 4 discusses the security problems at each IoT layer. Section 5 analyzes the solutions for the problems discussed in Sect. 4. Section 6 talks about the future directions, and at the end, Sect. 7 concludes the survey paper.

2 Related work

The related work comprised of various researches in the field of IoT regarding Intrusion Detection Systems. This portion is produced from the works proposed between 2005 and 2019 and was supported by scientific publications available in the scientific repository (IEEE Xplore, ACM Digital Library, Science Direct, Springer Link, Google Scholar). This production gives exposure to the works related to the specified topic. In this regard, the overview of various proposed research works is presented with respect to layer's security issues. Table 1 illustrates the work is done so far on the security issues and mitigation strategies according to IoT layer structure. In [40], Geneiatakis et al. discussed that the IoT system gives support to various types of applications such as smart industries, smart cities, and smart homes. Smart objects used in these applications interact with other components like mobile devices, data collectors, etc. to provide various services. While providing services, it also takes users to security and privacy threats due to their limited processing. So in this paper, writers put some light on some of the major security and privacy laws using off the shelf components. For this, they apply smart home IoT architecture and make users able to interact with it. Then, they analyze different scenarios for which they can easily identify possible security and privacy issues and proposed solutions for them.

Table 1 Comparison of existing surveys about smart home security issues and several solutions. ✓ shows fully covered, ✗ shows not covered and * shows partially covered

Ref.	Year	Topic	App. layer	Phys. layer	Net. layer	Percpt. layer	Security solutions
Geneiatakis et al. [40]	2017	Smart home	*	✓	*	*	*
Ali et al. [5]	2017	Smart home	*	*	*	✗	*
Zarah et al. [8]	2013	Smart home	*	✗	*	*	*
Arabo et al. [12]	2019	Smart devices	*	*	*	*	✓
Gendreau et al. [39]	2016	IDS	*	✗	✗	✗	*
Salman et al. [102]	2018	SDN	✗	✗	✗	✗	*
Zarpelao et al. [134]	2017	IDS	✗	✗	✗	✗	*
Pongal et al. [92]	2015	6LoWPAN and RPL	✓	✓	*	✗	*
Elrawy et al. [33]	2018	IDS performance parameters	✗	✗	✗	✗	*

Ali et al. [5] discussed that IoT is developing day by day and making a world where material things like smart cities, smart homes, etc. are pro-viding innovative and smart services to humans. Smart homes provide many services through Information Communication Technology (ICT). But due to its heterogeneous nature, it leads to some major security issues. So in this paper, they put the investigation on some of the attacks and check their impact on the overall system to predict accurate solutions. The main contribution in this paper is that the authors set some security goals, and according to that they predict how many attacks are expected to be launched in the coming years. The purpose of this research is to prepare well before the arrival of attacks. In [8], Zarah et al. proposed that due to rapid growth in IoT, smart homes have become one of the essential domains. Furthermore, it is an interconnected home where things interact with each other through the Internet. It is very beneficial for users and provides many facilities, but at the same time, it also faces many security issues which need to be resolved. A lot of research is carried out in which the researchers discussed these issues and presented different types of approaches to handle these issues. In this paper, we have analyzed the smart home approaches, security issues and also suggested the best possible solutions to make the smart homes secure from these types of attacks.

Arabo et al. [12] elaborated the trends and challenges of smart devices in smart homes through cyber security. They discussed that these smart devices provide some functionality to users. However, while providing more functionality, it also takes users to new risks and threats. In this paper, cyber security issues related to smart devices are discussed. They considered mobile malware is one of the main security issues in smart devices. They also predicted that in near future users can expect a large number of malware-related attacks due to mobile smart device, especially on the android platform. The main purpose of this paper is to highlight possible security threats in smart devices, secondly it discussed the challenges involved in mobile malware, and last one is to propose a security solution that can handle these types of threats. Gendreau et al. [39] discussed that IoT is the wide developing technology, but with this rapid development in IoT, it also faces many security problems. These problems become a barrier to high accessibility, reliability of the network, and security of data. In this paper, the authors projected Intrusion Detection systems (IDS) that are consuming the most original concepts to make IoT more sheltered and protected. They take start with the history of IDS systems from where they were initiated and how they are working these days. They also argued on many open-source problems that are encountered by IDS systems.

Salman et al. [102] discussed that the Internet presents Quality of Service (QoS) and associated security issues, but in the scenario of IoT, some of these challenges become more crucial. In this paper, the authors presented four leading IoT-specific challenges and also anticipated solutions to the problems that help to resolve these challenges. The proposed SDN-based solutions are combined with fog computing. This is because SDN has a universal observation of network and can present more efficient solutions to make them secure, but on the other hand, fog computing is used to bring cloud in the network. By this, the network becomes scalable and more responsive. Zarpelao et al. [134] deliberated different kinds of security issues which IoT is facing and discussed that there are many techniques that are used to eradicate these issues to protect IoT devices. But from these techniques, many of them are occasionally susceptible to numerous attacks. In this survey paper, the authors anticipated IDS to detect different kinds of attacks. They proposed IDS system because they found that this technique is pretty supportive to protect IoT. They also explained how different kind of open issues is becoming a hurdle to IDS expansion and what are the solutions to those issues.

Pongal et al. [92] discuss that 6LoWPAN is an IPV6 header compression protocol that can straightforwardly become the target of the attackers. To handle these attacks, RPL is designed, which is a network layer routing protocol. RPL is a lightweight protocol and can also go under attacks. So in this paper, they emphasized multiple attacks that were dangerous for both RPL and 6LoWPAN. They also provided countermeasures toward these attacks to make a secure network. They also discussed consequences that may occur due to the network parameters after applying solutions. Furthermore, they also intimated that there are many attacks on RPL which are not evaluated yet. Elrawy et al. [33] carried a survey about IDS. In this work, they surveyed the IDS as a security solution for IoT. In this work, various designs and approaches of IDS are presented which are operating in the IoT environment. They mainly focused on the performance factors of IOT equipment, such as accurate detection, energy consumption, time taken for processing, and performance overhead. They also covered to some extent IoT systems, what is a smart environment, and an overview of IDSs. Furthermore, it is also discussed that traditional IDSs are failed to work properly against security attacks due to IoT network variety and protocols. They also provided future recommendations on the strengths and weaknesses of current IDS.

Robles et al. [99] deliberated that a smart home is a home in which things are connected to the Internet to provide benefits to the users. Despite having some advantages, it also has many disadvantages and security is one of the most important of them that is still unresolved. It is very difficult to make smart homes secure. In this paper, the authors discussed the tools and techniques used in smart homes and also reviewed the tools used to make smart home security to provide security. Konidala et al. [70] anticipated that the concept of smart homes is becoming more popular due to its easiness to the users. In this environment, Radio Frequency Identification (RFID) technology is very essential to use. There are many RFID approaches used in the smart homes but in this article, they used some of the more beneficial techniques for smart homes and suggested it as their proposed approach. From the techniques, the authors identified privacy and security threats and also proposed a secure approach. In the end, the authors claimed that their approach is just a conceptual idea. Bastos et al. [19] researched that with the start of Google devices and Amazon Echo family, IoT devices used in the home are increasing rapidly. It also has afterthoughts for security and privacy. So due to this, malicious actors can easily attack these devices and make damage to the users. Authors also researched that DDoS attacks are easy, that occur on IoT devices, and have huge destructive consequences. This paper is a comprehensive survey of IoT which includes technologies and security issues. They take those issues which were focused on the smart home. They also discussed possible solutions which can be used to protect IoT from various kinds of attacks.

Bugeja et al. [20] discussed that smart home is becoming popular day by day due to IoT products, to provide quality of life to individuals. Though this is a heterogeneous environment where every device is connected to another device in this network. So by this behavior, it has security and privacy issues. Making smart homes secure becomes a very crucial topic and needs more research to solve these security issues. In this paper, they presented an overview of privacy and security challenges that are related to a smart home. They also discussed various kinds of solutions to these challenges and also deliberated those challenges which need further research to be resolved. Islam et al. [53] discussed that Wireless Sensor Network (WSN) is becoming popular to improve quality of life in IoT-based smart homes environment. Sensors are used to monitor the position of occupants. Sensors also cooperate with themselves to deliver information. Ensuring privacy and security provided by WSN is one of the major issues in the smart homes domain. So in this paper, they search for the privacy and security issues in smart homes. They also discussed unique problems that distinguish other applications to smart homes. They also elaborated on those issues which require further investigation for a solution.

Kominos et al. [69] deliberated that these days electricity industry has become a hot topic due to the evolution of electrical grids to smart grids. Initiative in this evolution led by industry and academia is also facing some issues. In this survey paper, issues in smart grid and smart homes which are an integral part of smart grid are discussed. They presented some of the threats to smart homes based on several scenarios. They set some specific goals for smart homes and then they categorized these threats according to those goals. Lin et al. [79] proposed that IoT is a single domain problem with solutions that are applied to almost all kinds of IoT applications. However, privacy and security need more attention to be resolved to protect the smart home environment. Financial and human resources are working together to improve security issues. Technical issues are important but human issues also need consideration to be handled as crucial. After studying the existing solution to improve IoT security, the authors identify some of the main requirements in smart homes that are important in the future. For this purpose, they used gateway architecture which is most appropriate for high system availability.

Yoon et al. [133] anticipated that IoT is one of the most evolving technologies in almost every field but in the smart home, it is growing rapidly. Enterprises enter the smartphone market due to the development of mobile networks. However crucial incidents can happen to IoT applications because they provide services without considering security. So in this paper, they analyze some of the main security issues in Smart Home and also propose a solution to countermeasure these issues. In the aforementioned related papers, security challenges are not discussed in terms of the layer's structure. Several articles only discuss a little bit about layers and give no solutions regarding the security challenges against target layers. This work surveyed the IoT environment, how this technology is spreading. Specifications of different smart home devices are also included. In this paper, the IoT environment is presented in the form of layers.

3 Internet of Things (IoT)

In 1999, Massachusetts Institute of Technology (MIT), for the first time, brought the concept of IoT. In recent years, the IoT paradigm has become more popular. IoT comprises different hand-held devices like smart phones, tablets, laptops, personal computers, and other embedded devices like smart watches, smart doors, smart locks, etc. as shown in Fig. 3. In IoT, devices communicate without human interaction. All data is sent and processed automatically according to the situations, for example, if some place catches fire, then all the sensing devices start communication according to the scene. Fire sensors sense the fire and trigger an alarm to activate other supporting devices to wipe out the fire.

IoT is the collection of multiple devices, which makes it a heterogeneous environment. To achieve the objective of IoT, we have to organize the environment in such a way that all devices should work perfectly. Table 2 shows a depiction of trends in advancement in smart home technologies. Due to heterogeneity, various problems arise in IoT paradigms like formalization problems, standardization problems, data problems and security. To obtain a successful transaction, all smart nodes and Radio Frequency Identifier (RFID) equipment should be connected reasonably. In formalization, users focus on reliability (should cover all aspects), optimality (should use minimum numbers of nodes) and redundancy (fault-tolerant, portable and easy recovery from mishap).

In IoT, every single node or protocol needs to be standardized. To overcome the heterogeneous nature of the IoT environment, the entire network should invent a worldwide standard to work with other equipment smoothly. As data is like a skull in the IoT network, thus, it is necessary to ensure the integrity and availability of the data. It should circulate from legitimate devices and sensor nodes and make sure that there is no pirated device within the premises of the IoT network. Figure 4 shows trends of research studies on the security issues of IoT devices. It shows that

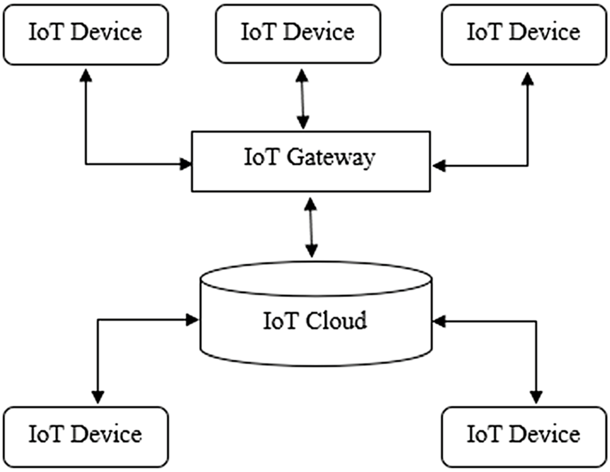


Fig. 3 IoT structure

Table 2 Advancement in IoT technologies

Technology	Data rate	Frequency	Year
3G [35]	50 Kbps	1.8 to 2.5 GHz	2002
4G [35]	2 Mbps to 1 Gbps	2 to 8 GHz	2010
5G [35]	1 Gbps or Higher	3 to 300 GHz	2015
Bluetooth [91]	700 Kbps	2.45 GHz	1999
WiFi [126]	2 to 54 Mbps	2.5 to 5 GHz	2000
RFID (radio frequency identification) [98]	2 to 100 Kbps	125 to 2.45 GHz	1948
BLE (bluetooth low energy) [120]	1 Mbps	2.4 GHz	2010
LoRaWAN (low-power wide area network) [83]	50 Kbps	500 to 125 KHz	2015
WLANs (wireless local area networks) [103]	100 to 125 and 540 Mbps	2.4, 3.6, 4.9, 5, and 5.9 GHz	1997
Z-wave [88]	9.6 to 100 Kbps	908.42 MHz	1999
Sigfox [18]	100 bps	100 Hz	2009

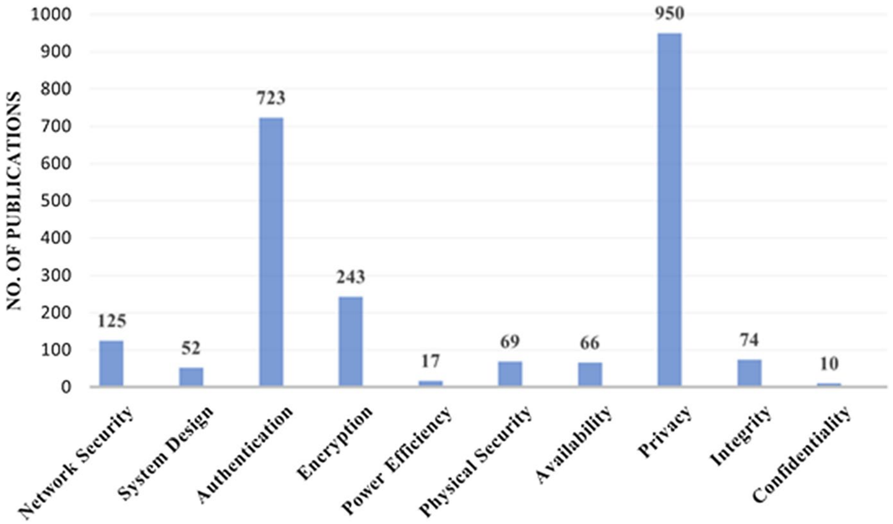


Fig. 4 Trends of research studies on the security of IoT devices

a comprehensive research is done on the privacy and authentication issues, however, there is dire need to carry out research with respect to confidentiality issues and to make IoT devices energy efficient.

IoT faces various security challenges from different aspects, like communication protocols and hardware equipment. IoT devices have less memory, short battery time, which causes them to own low computational power devices. Gateways connect IoT devices to the outer world which may cause security issues. A compromised node may cause an information breach. An intruder can cause issues by manipulating a device physically. A natural disaster can damage IoT devices, which may produce any security threats. Network layer would be vulnerable to a plethora of security issues as it plays a critical role in the IoT environment. Figure 4 shows the architecture of the IoT network. The gateway acts as a threshold between IoT devices (smart A.C., smart locks, smart lights, smoke sensors, and noise sensors) and control devices (laptops and user's mobile phones). Controlling devices and IoT devices are connected through the cloud.

3.1 IoT layers structure

Figure 5 illustrates the layers architecture of the IoT environment. These layers accomplish the objective of IoT [85, 111]. Below are the main layers that take part in the IoT objective.

3.1.1 Application layer

All the applications and services that IoT provides, such as smart cities, smart homes, smart hospitals, and intelligent transportation, reside in the Application Layer. The application layer is one of the top essential layers which has to demarcate all applications, where the IoT system is deployed. It acts as an interface between network and IoT devices. This is the layer, which has the authority to confirm applications are gaining services or not. It also has the authority to deliver different services to different applications according to information gathered by sensors. It has many issues, but still, security is on the topmost of the list [130].

3.1.2 Perception layer

Different devices or technologies that perceive input from the environment are part of perception layer. These devices and technologies are pressure sensors, smoke

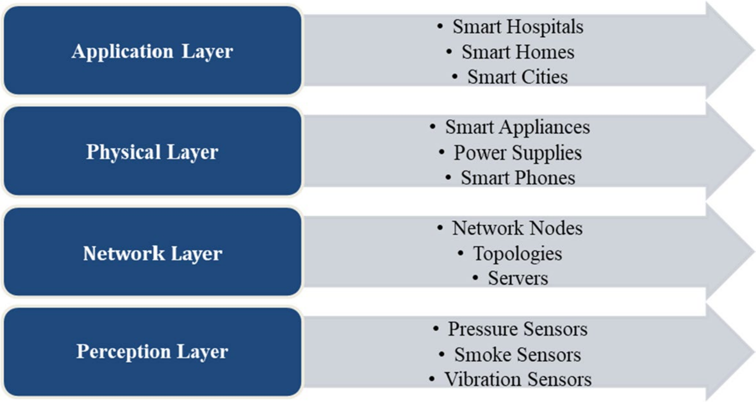


Fig. 5 IoT layers structure

sensors, vibration sensors, and RFID sensors. The main function of the perception layer is to bring together modestly process information, which is a fragment of a scholar. It is also recognized as an extension layer. Numerous problems exist on this layer. The main problem which has to be resolved is collecting and capturing information [65].

3.2 Network layer

The network layer consists of network communication software (like topologies) and network devices (like servers and network nodes) that help different devices to communicate with each other. It is also acknowledged as a transmission layer. The key feature of this layer is to send data to end devices and the devices in between the end nodes. It is established on mobile telecommunication and the Internet. One of the foremost persistence of this layer is to deliver information through extensive distance. In other words, it acts as a bridge. The main objective of this bridge is to transport data from objects through sensors. The medium provided in this layer can be wired or wireless. Networks and network devices are associated with each other through this layer [123].

3.2.1 Physical layer

The physical layer comprises hardware devices or physical components like power supplies, smart appliances, and smartphones. These are the backbone of the IoT world. This layer comprises sensors that help in sensing the environment, consequently gather information from the environment. This layer also senses other objects in the environment [105]. IoT environment involves smart devices and Internet connectivity. Every connected device communicates to another device to perform the desired task. Smart devices include laptops, personal computers, mobile phones, tablets, smart A.C., smart TV, and other wearables. Table 3 shows the different devices and their specifications that take part in IoT-based smart home.

4 Smart home problems

The adaptability and deployment of IoT technology are increasing day by day, thus, more and more smart devices are connected to the Internet [112]. As discussed in Sect. 3, the IoT environment is based on four layers. Thus, to ensure the security of the smart home, we must deploy security at each layer. Figure 6 depicts a smart home layout in which smart devices are connected to a gateway that connects the devices to the Internet. The gateway acts as the bridge between the Internet and smart devices. Various security attacks are also highlighted in Fig. 5 that show how an intruder can take advantage of security vulnerabilities and hijacks the network. In addition, the security issues related to each layer are discussed. Furthermore, an overview of the security challenges at each IOT layer is highlighted in Tables 2, 3, 4, and 5 along with the solution of each problem and tools/techniques.

Table 3 Smart devices with specifications

Sr.	Device type	Chipset	RAM (GB)	Power	Network protocol	Flash memory (GB)	Core Freq. (GHz)
1	Wink hub 2	ARM cortex-M3	0.512	Battery	Wi-Fi 802.11	0.064	1
2	Samsung Smart things hub	ARM cortex-A7	0.256	Battery	Wi-Fi, Bluetooth	4	0.528
3	Amazon echo	ARM cortex-A8	0.256	Battery	Wi-Fi 802.11	4	0.8
4	Philips hue	Ambiance A19	0.004	AC	Wi-Fi 802.11	64	1.7
5	TP link HS200	AR7240	0.032	Battery	Wi-Fi, bluetooth, NFC	0.04	0.4
6	Ecobee4	AMD A4-9125	4	Battery	Wi-Fi	1000	1.7
7	L.G. smart TV	ARM cortex-A53	2	Battery	Wifi, bluetooth	8	1.1
8	Samsung smart cam	Micro SDXC	N/A	AC	Wi-Fi, NFC	32	Up to 0.54

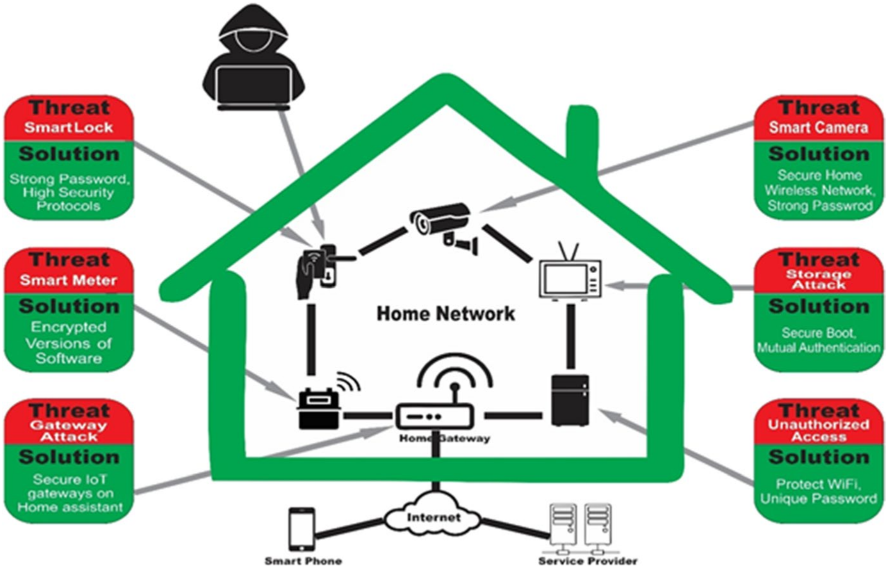


Fig. 6 Smart home architecture

Table 4 Application layer security issues

Sr.	Application layer security issues	Solutions	Tools and techniques
1	Vulnerable software	N/A	N/A
2	Phishing attack	[44]	Visual similarity and data mining
3	Manipulation of an unstable configuration	[97]	Markov model
4	Reconfiguring remote devices attack	[50]	Point to point encryption
5	Social engineering attacks	N/A	N/A
6	Hacking into the smart meter/grid	[64]	Rabin encryption cryptosystem
7	Malicious code attack	[125]	Status-based detection
8	Attacks on access control	[115]	Role-based authentication
9	Tampering with node-based applications	[55]	Proactive digital forensics, Holochain and fog computing
10	Failure to receive security patches	N/A	N/A

Table 5 Perception layer security issues

Sr.	Perception layer security issues	Solutions	Tools and techniques
1	Eavesdropping	[24]	Visible light communication
2	Sniffing attacks	[31]	N/A
3	Booting attacks	[81]	Field programmable gate array
4	Node capturing	N/A	N/A
5	Side-channel attacks	[121]	Rekeying and masking
6	Noise in data	[135]	ANR (automatic noise reduction)

4.1 Application layer security breaches

The application can be aborted or can be used in the wrong way due to fade security. Consequently, the application fails to accomplish the needs for which it is to be programmed. As a result of the attack, this layer can produce bugs in the application program that leads it to function abnormally [72, 112, 132]. Below are common threats at the application layer. Table 4 gives an overview of the attacks in the Application layer.

4.1.1 Phishing attack

In this attack, the intruder gets access to the network using the email of high-ranking personnel of the organization. Attackers get access to sensitive information and may damage the confidentiality of the organization which may lead to huge losses [113]. In [89], Nirmal et al. discussed that these attacks are most anticipated in the devices that are connected to the Internet. This attack is on the rise for the past few years. The reason of this rise is that attackers are encouraged with a huge amount for the stimulation of the attacks. Numerous authors declare phishing as identity theft because the attacker confuses the visitor either by providing an identical web page to the original one or pretend himself as a legitimate user [95, 128, 131].

4.1.2 Malicious code attack

This type of attack can be a malicious worm circulating over the Internet that can hit the embedded devices running a particular operating system such as Linux. Such a worm can target a range of small devices having an Internet connection, like security cameras and routers. This could also break into the car's WiFi and take control over the steering wheels and let it crash, resulting in several injuries to the innocent [28]. In [125], Dongdi et al. discussed such kind of attacks and summarized into three categories. Botnet Mirai attack falls in the category where intruders listen to the network activity and sniff the traffic [45]. Ransomware attack is a type of malicious code that sends packets either for attack or communication. It gets access to the application and spreads itself into the victim application. Consequently, it encrypts the target system and at the end locks the system [107]. The last category deals with hardware or sensor manipulation [136].

4.1.3 Tampering with node-based applications

Hackers get control over the application of the device nodes and install malicious rootkits. The security design of smart home devices should be tamper-resistant or able to warn about tampering. It is not enough to protect some key parts and left others bared for security attacks. Some threats can change the behavior of the devices, and it functions abnormally, like a tampered temperature sensor would not change its temperature value and rely on showing some fixed value [22, 50]. Pal et al. [116] termed tampering as the physical modification of IoT components by the attackers. As a result of this filthy action, the intruder may steal the identity of a legitimate user, or hardware components may be replaced with a compromised one.

4.1.4 Attacks on access control

The IoT environment is thoroughly confidential. Any compromised device or person can damage the confidentiality, and the entire environment becomes vulnerable to various attacks. Access control is a process that ensures only a legitimate person can access the data [47]. According to Bhawna et al. [3], access control attacks take place when an authentic procedure for access control is violated. This procedure gives permission to only authentic users, processes, or applications to use the system. Access control attack is one of the critical attacks. Once access control is compromised, then the whole system becomes vulnerable to attackers [47, 137].

4.1.5 Failure to receive security patches

In sensitive areas like, nuclear reactors, the bug inside the mobile node is not updated with software patches, which may end up with devastating results. Smart phones and computers get an automatic update but some IoT devices fail to adopt this service, ultimately become vulnerable. From another perspective, the device shares its backup during patches update and as a result, faces a slight downtime. During downtime connection may be unencrypted, hence intruders can hijack sensitive information during this interval [27, 66, 68].

4.1.6 Hacking into the smart meter/grid

Utility bills of smart homes are dynamically generated through the smart meter; it sends the usage of the power consumption and other resources to the concerning authorities. So, it must be secured because one can track the availability of the person in the home based on power consumption. So, this can cost billions of dollars [37]. In [124], Zhiwei et al. define smart meter attack as the duplication of the authentic smart meter by the attacker. The irrelevant data shared by the compromised meter consume the bandwidth for no purpose.

4.1.7 Vulnerable software

Programs written by less skilled programmers are normally not up to standards. Thus, nonstandard programs become vulnerable to security attacks. Attackers can easily break the security of such software. IoT devices shipped with default settings and authentication free operating system create a security gap for intruders to modify the built-in setting and operate the device for malicious activities.

Software installed through third-party resources or by cracking license is easily compromised by intruders [9, 96, 127].

4.1.8 Manipulation of an unstable configuration

Usually, in the IoT environment, several components like remote servers, operating systems, and storage servers are used for running IoT applications. It is quite possible that these services are configured improperly and may lead to security issues in the application layer [1].

4.1.9 Re-configuring remote devices attack

In some cases, IoT network devices are reprogrammed remotely through a network programming system. An insecure network programming system can easily be hijacked by intruders and can damage the IoT environment. While configuring devices far from the physical location, programmers have a deficiency of spontaneous communication that can lead to problems [87]. In some cases, IoT network devices are reprogrammed remotely through a network programming system. An insecure network programming system can easily be hijacked by intruders and can damage the IoT environment [2].

4.1.10 Social engineering attack

In social engineering attacks, victims are humans instead of network devices. Users are attacked psychologically. In social engineering, the attacker communicates directly with the victim and tries to provoke user to leak sensitive information like credit cards. The attacker demands the information that can lead to a huge attack or asks the victim to visit some website for phishing purposes [41, 48, 106]. In [42], Ghasemi et al. termed social engineering as the social interaction mechanism to convince the victim (maybe a person or an organization) to commit nasty activities according to the instruction given by the intruder. Social Engineering attacks are divided into two types. One is human-based, carried out face-to-face. The second one is computer based which is a cyber-attack.

4.2 Security problems in the perception layer

Hackers target the node level, as these are a buildup of sensors and are favorite to hackers. Hackers make use of these to replace the device software with their own. Mostly threats at perception come from outside entities and the devices with sensors play a key role to make it happen [47, 60, 104]. Table 5 summarizes perception layer's issues. Some common issues in the perception layer are discussed below.

4.2.1 Eavesdropping

The devices inside the smart home communicate with each other and also with the server through the Internet. This can lead to eavesdropping because these devices are usually left unattended. In this case, trustworthy devices can send push notifications to the smart home user and would be able to gather confidential data [24]. In IoT networks numerous types of devices are communicating with each other through a local communication station in which a third party can involve and access their private information and this procedure is known as eavesdropping [63].

4.2.2 Sniffing attacks

Attackers collect private information by putting down malicious sensors or devices in the vicinity of the actual devices in the smart home network [36]. Vashi et al. in [117] discussed that an attacker can force an attack to enter into the system as a sniffer application. By this, users don't know about the attack and the attacker can easily steal their private information.

4.2.3 Booting attacks

In edge devices, built-in security mechanisms do not work at the time of the boot process. During this process, devices become vulnerable to various security attacks. Attackers take advantage of this weakness and target the devices for their malicious purposes. Therefore, it is essential to make devices restive against vulnerabilities during the booting process [47]. A booting attack is applied at the start of the system when devices are getting ready to communicate or security algorithms are not installed yet. Through physical communication protocols, the attackers can do their job even if devices are not in communication mode. These protocols are UART or JTAG [38].

4.2.4 Node capturing

IoT network comprises several devices and low-power sensors. Attackers can easily target these fragile sensors. A compromised sensor can bypass information to rivals; therefore, attackers tend to replace network nodes with their own to capture information. This malicious node pretends to be a trustworthy device but works for attackers [74]. According to Garva et al. [38], in this type of attack an attacker takes control of a sensor that is observable in the system but instructed by the attacker. This may work as a gate for the attacker to enter into a system. In this way, an attacker can harm the network or steal the private information of users.

4.2.5 Side-channel attacks

Side-channel attacks are another source of leakage of sensitive information. Factors like power usage, architecture, and way of communication of sensor devices expose information to attackers. Side-channel attacks are triggered through power usage, timing attacks, electromagnetic attacks, and laser-based attacks [47]. According to [25], side-channel attack is one of the most famous techniques to breakdown the safety of an encrypted system. It breaks the security by using valuable information that is escaped by the physical devices.

4.2.6 Noise in data

As devices in the smart home are connected through a wireless medium, so when data cover a significant distance, it is quite possible that it can contain incomplete, irrelevant, and false information. Such irrelevant information can cause smart home devices to perform unwanted or even worse actions that can lead to harmful results [108]. Noise in data in IoT means that it is a threat to the sensor's data. As the devices are connecting increasingly to the network, this problem is also rising with them. Electric components that are inside or outside of the IoT devices cause this type of noise [46].

4.3 Security issues in the network layer

The network layer is responsible for the exchange of information between the devices. As a result, congestion of data also occurs at this layer. The main security issues of this layer are the integrity and authentication of data that is to be delivered to concerned devices. Prominent security risks over the network layer are discussed below. Table 6 gives an overview of attacks in the network layer.

4.3.1 DoS attack

A large amount of data is sent to servers or devices; as a result, those are unable to respond to anything other than this bombarded data. An overflow of data is sent over the channel, and it produces congestion over the link, and the sender

Table 6 Network layer security issues

Sr.	Network layer security issues	Solutions	Tools and techniques
1	DoS attack	[62]	IDS framework
2	Gateway attacks	N/A	N/A
3	Unauthorized access	[80]	Role-based access control authorization
4	Storage attacks	N/A	N/A
5	Man-in-middle attack	[6]	IDS and IPS (instruction prevention system)
6	Injecting fake information	[7]	Multi-factor device authentication
7	Data transit attack	[71]	Multi-factor device authentication
8	Black hole attack on RPL	[135]	Multi-factor device Authentication
9	Hello flood attack	[61]	Multi-factor device authentication

and receiver become dumb [104]. When a DoS attack occurs, it shuts down the network and the user's access is denied. It achieves this by allowing the food to track on the target or sending the information that did a crash. In both cases, it takes the access of users from the service they expected [13].

4.3.2 Gateway attack

This attack tears down the link between smart home devices and the Internet. It could be a DoS attack, or routing attacks rose in a gateway end up with null or misinformation sent to smart home devices like sensors, actuators, and nodes from the Internet [60, 73, 118]. According to Ande et al. in [10], a gateway attack demolishes the link between the sensors and the ISP. Consequently, the sensor data vanished on the link or redirected. Thus, it gives birth to the DoS attack.

4.3.3 Unauthorized access

If the smart home devices are left open and the owner expects that these are in safe hands. These devices can be accessible by unauthorized users. An unauthorized user can use these sensible devices for filthy purposes [15, 30, 94]. In [49], Hossain et al. discussed that unauthorized access to the medical environment is horrible, as it can kill the patients. Unauthorized access to actuators or sensors can manipulate the patient's records which can damage the precaution cycle. Hussain et al. discussed in [51] that unauthorized access to the RFID nodes can lead to information leakage. The intruder can get access to the sensitive information and possibly alter the node information. When an attacker gets access to the RFID nodes, he can easily read or write the node information. This phenomenon may lead to further fatal attacks on the IoT network.

4.3.4 Storage attacks

A massive amount of data and valuable information is stored on the cloud or storage devices; both can be accessed and can be changed to irrelevant information. Duplication of data, along with access to numerous users, increases the chance of being attacked. A large amount of users data is stored on storage devices and the cloud, both can be easily attacked by the attacker, and consequently, the user faces a huge loss of precious data [14, 14, 16, 32].

4.3.5 Man-in-middle attack

In this type of attack, the attacker does not bother to be physically present at the victim's place. The attacker gets the information through IoT protocols. By using protocols, he disturbs the communication between two devices and collects desired information [96]. According to Kim et al. in [67], this type of attack, the malicious actors (attackers) create a hurdle between the communication of two systems. They can get access to the information that these two systems were trying to share. In this way, the attackers can steal the private information of these systems.

4.3.6 Injecting fake information

Harmful people can inject irrelevant information in the system, causing it to function abnormally or produce unexpected results [73, 108]. Samah et al. in [59] discussed that in wireless sensor networks intruder target a node for manipulation and then inject irrelevant information into the network. This makes the network vulnerable to numerous security attacks.

4.3.7 Data transit attack

A large amount of information exchanges among IoT applications, like sensors, actuators, and storage servers. Data is the most valuable asset of any user and thus attackers always target confidential data for malicious purposes. Stored data has a security risk, but the type of data between communication channels has maximum chances to become vulnerable. Along with sensor devices, different technologies are used in the information transfer, which increases the chances of making the IoT environment a data breach [47].

4.3.8 Black hole attack on RPL

The black hole attack is initiated by a compromised device that aims to disturb the network track. It distorts the network track by dropping the packets that are routed through it. This attack cannot be detected easily, as the attacked network behaves as a whole network. Black hole attack is only carried out on ContikiOS and RPL (Routing protocol for lossy network) [129]. Other operating systems like Tiny O.S., RIOT OS are not vulnerable to this attack.

4.3.9 Hello flood attack

Hello flood attack occurs in the network layer. In this attack, the intruder captures a node and sends hello messages to another node, and declares itself as a neighbor of receiving nodes. Due to the high power of messages, the receiver considers the compromised node as the nearest base station and starts communication with these malicious nodes [90]. This attack is happened by a node that sends a packet called hello packet with high power. Because of very high power, the nodes of the network and even out of the network considered it as a parent node. Then, all communication and messages are routed through this parent which can cause damage for the users [43].

4.4 Physical layer security breaches

Power supplies are the backbone of smart home devices. There must be such a mechanism through which these devices can survive during a power interruption. At this layer, devices must be kept safe from the weather and the individual. New technologies should be implemented to ensure the safety of power resources and physical attacks [72, 112, 132]. Table 7 summarizes Physical layer's issues.

Table 7 Physical layer security issues

Sr.	Physical layer security issues	Solutions	Tools and techniques
1	Physical damage	[122]	Puf-based protocols
2	Environmental attacks	N/A	N/A
3	Loss of power	N/A	N/A
4	Hardware failure	N/A	N/A
5	Jamming	[61]	Identity verification protocol
6	Malicious code injection	N/A	N/A
7	Duplication of a device	[110]	SDN-based approach
8	Overloading RFID	N/A	N/A
9	Duplication of tags	[63]	Quantum key distribution

4.4.1 Physical damage

This may be a direct approach of attackers to damage the physical devices of the smart homes, like, sensors, nodes and actuators. Consequently, these devices are unable to take part in the network and failed to work smoothly [17]. According to [52], this may concern with physical devices which can occur by a malicious actor of abnormal environment. By this vulnerability, the devices may lose their functionality and can generate other risks.

4.4.2 Environmental attacks

Environmental attacks can also damage the network devices. Like a sensor may get affected due to rain, storm, or snow. As a result, it may lose its functionality and unable to work properly and hence causes more problems. These types of attacks affect sensors by environmental hazards like an irregular storm, rain, etc. By this irregular behavior, the sensors may lose their functionality [11, 84].

4.4.3 Loss of power

Network devices rely on power and in the absence of backup power resources, these devices automatically go to power-saving mode. Loss of power attacks does not let the device go into power-saving mode, consequently, devices use more power and soon become faint. Kalra et al. [57] elaborate that the devices that lose power accidentally are not able to work normally and cannot provide services. It is a common strategy that a device may save power by entering into the various power-saving modes, but sleep deprivation attack becomes a hurdle between the device and power-saving modes [56].

4.4.4 Hardware failure

In smart home, users are much more dependent on the hardware devices, so they cannot think of hardware failures. If a hardware failure occurs, then devices start behaving worse by sending erroneous information. The impact of hardware failure is directly associated with network failure [21]. According to [109], a network is failed and unable to do its job if any of the device in a network faces failure.

4.4.5 Jamming

In jamming, radio signals are bombarded on the victim network or device to disturb the communication. Much thicker jamming can paralyze the entire network. Due to jamming, battery drain rate of the devices increases as it has to re-transmit the data due to disrupted communication [29]. In [114], the authors discussed that jamming is one of the most dangerous security attacks in wireless sensor network (WSN)-based IoT. By blocking the channel, it breaks the circulation of a network. An attacker can easily jam the track on the wireless channel.

4.4.6 Malicious code injection

In this attack, malicious software is injected through the debugging interface. As the device with injected software is already in the network, it can disturb the entire smart home environment by pretending to be a trustworthy device. Furthermore, sensitive information on a protected network may be sent out through this injected malicious software device [11]. In [117], Vashi et al. analyze that malicious code injection is one of the most destructive attacks in which an attacker can inject malicious code into a network. By this, the network shuts down its working or in the other case, the attacker controls the entire network and can steal any type of data from the network.

4.4.7 Overloading RFID

To interfere with the RFID function, a huge amount of noise signal over radio frequencies is sent by an intruder. In this way, RFID is unable to function normally [75]. According to Said et al. [101], RFID uses a metal surface. By using this, tags in RFID are unable to transmit information to the device and also tags are not able to receive power.

4.4.8 Duplication of a device

Features of a genuine network device can be changed by malicious manufacturers, like hardware, software, and configurations. The affected device could run malicious software to target genuine device or damage the operations of other network devices. A malicious actor (like an attacker) makes a clone device in an IoT network. By that device, they have almost full access to the network and consequently damage the network [23, 100].

4.4.9 Duplication of tags

Intruders can easily capture the tags that are deployed on different objects. Attackers produce clones of such tags and deceive RFID readers by compromising the RFID system. All the objects having tags on them are vulnerable to physical attacks [86]. According to Datta et al. [26] in particular RFID systems, the attacker tries to understand the security protocols. With this information, the attacker tries to blank the tags by writing received data in the same format.

5 Solutions of smart home's problems

This section discusses the security solutions for each layer. IoT's four layers, discussed in the previous section, experience numerous security attacks that may cause serious loss to the user of IoT. Solutions to such problems are necessary; otherwise, users will be reluctant to use IoT's services. Solutions are organized according to each security layer. Table 8 illustrates the comparison of various research works that provide the solutions of smart home issues. This table shows tool and techniques used by different researchers.

5.1 Application layer

The application layer is responsible for the services delivered by the IoT environment, such as smart cities, smart homes, smart hospitals, and intelligent transportation. Such applications can be elected, or an intruder may use them in a nasty way to harm the masses. Consequently, the application fails to accomplish the needs for which it was programmed. Solutions for the application layer's problems are discussed below.

5.1.1 Fighting against phishing

Gupta et al. in [44] proposed various schemes to fight against phishing like network protection based on blacklist scheme, or schemes such as heuristic, in which erroneous emails are blocked either on client-side or server-side. Users should be educated to such an extent that they can differentiate between a phishing website and a normal website. Other solutions like network-level protection and user authentication can help to diagnose phishing attacks.

5.1.2 Malicious code detection

IoT devices have less computation power and can't run on heavy malicious code. Wei et al. in [125] used a collaborative detection strategy is to detect malicious

Table 8 A summary of security solutions

Refs.	Objective	Tools and Techniques	Benefits
[44]	Phishing attack solution	Classification	Twofold, phishing attack and taxonomy of phishing attacks
[125]	Solution for malicious code	Microduino Core+ and Sniffing code	The running status of the monitoring device can detect malicious code
[77]	Eavesdropping solution	Channel Randomness model	Eavesdropping attack has a beneficial impact of shadow fading effect
[4]	Solution for black hole mitigation	RPL protocol and Mitigation technique	Packet delivery rate is increased and effectively detect black hole attack
[80]	User authentication’s solution	RBAC-based authorization scheme	Prevent various attacks like eavesdropping, MIM, replay, key control attack, etc.
[133]	Data Encryption’s solution	CP-ABE scheme	Guarantees data security and during the data retrieval process provide user privacy
[135]	Solution for noise avoidance	Automatic noise reduction algorithm	Performance of ANI from UCI data repository is evaluated
[6]	Solution for MIM attacks	OMNET++ and IPS IDS scheme	Lightweight and strong encryption technique
[58]	Solution for tag cloning	Modified count-min sketch vector	Reformed count-min draught vector and dual hash collisions
[61]	Protection of Hello flood attack	Identity Verification Protocol	The first analysis of secure routing in sensor networks
[110]	Network-level security’s solution	VeloCloud and SDN principles	Identifies and block threats at network level
[78]	The solution at the perception layer	PKI-like protocol and security architecture	Corresponding mechanism PKI-like is improved
[62]	Solution for DoS attack	IDS framework	Characterizes an encouraging clarification for certifying better security in 6LoWPANs

codes. The strategy used by this approach is to analyze the normal running time and abnormal behavior when malicious code is deployed.

5.1.3 Tamper resistance

IoT devices should be designed as tamper resistance. Sensors that can detect tampering should be deployed on devices. If devices are not tampering with resistance, they should be kept in a secure place where devices are inaccessible for irrelevant people.

5.1.4 Conjure role base access control

In role-based access control, any person or entity of an environment has access to specific devices according to his role. Only specific resources are accessed by a person related to his role. A central system is responsible for assigning roles, adding new devices, and securely removing expired devices.

5.1.5 Secure smart meter

Gawade et al. in [64] used Rabin encryption that helps to ensure that data is sent to legitimate authorities, and data delivery is safe from attackers. The sensor should be deployed to make the meter tamper resistance and measure the parameters (current, voltage) regularly. A certain threshold can be fixed to avoid the overflow of parameters.

5.1.6 Countermeasure of misconfiguration

IoT devices should be shipped with up to date software and replace with devices that are running outdated software. As in the IoT environment, heterogeneity exists; therefore, inter-operable devices can reduce the chances of misconfiguration.

5.1.7 Countermeasure of remote reprogramming attacks

User authentication ensures that only legitimate user can reprogram devices through the remote source. Ant-replay protocol, which is a subprotocol of IPSec, prevents the network packets by an intruder to make changes in packets.

5.2 Discussion

The application layer is responsible for providing IoT services. This layer experiences numerous security issues. To work smoothly, it is necessary to overcome such security vulnerabilities. To educate people regarding security threats, various solutions are extracted from different proposed works. To fight against phishing blacklist and heuristics schemes are used. For the blockage of malicious code, a collaborative detection strategy is carried out. Tamper sensors are used for the sensing of tampering. To limit access to the system Conjure Role Base is adopted. Smart Meter ensures the delivery of the data to the legitimate authorities. To avoid the misconfiguration issues up to date software are necessary for IoT's equipment. Remote programming attacks controlled by anti-replay protocol.

5.3 Perception layer

The perception layer is comprised of the devices that act as sensors in IoT. Information perceived from the environment is a thorough production of the perception layer. This layer needs much security compared to other layers. Several security solutions regarding the perception layer are discussed below.

5.3.1 Security against eavesdropping

Li et al. in [77] proposed a system in which activities of eavesdroppers are monitored. In this work, channel specifications are known in advance, and different antennas are also deployed. For analysis purposes, a formal analytical model is proposed by taking into account different effects like path loss effect, shadow fading effect, and Rayleigh fading effect [24].

5.3.2 Sniffing detection

To avoid sniffing, the devices should be connected to trustworthy networks and must not be connected to public places network. WiFi offered by public places is not monitored properly and may contain bugs. Attackers sniffing these networks or build a new network on their own and use names of public places such as Free Airport WiFi and Free Bus Stand WiFi. Nearby users connect with this malicious node and send data through this service. Encryption plays an important role in securing network track that encrypts all the data which leaves the IoT system. However, data capture intruders would not make sense of it.

5.3.3 Secure boot process

Insecure boot process when the device is turned on, it operates cryptographic code signing techniques. A code developed by a trustworthy vendor or original equipment manufacturer (OEM) is executed on the device. By utilizing a secure boot mechanism, one can minimize the chances of replication of firmware code by an attacker.

5.3.4 Defensive mechanism against side-channel attacks

On the hardware level, information-aware hardware, randomization, and partitioning are used to prevent information leakage. On software-level algorithms like leakage-resilient public-key encryption scheme is run that guarantee the confidentiality of information even when some bits are lost.

5.3.5 Noise avoidance

A certain mechanism is used to eliminate noise in data. A neural network can help most effectively. In [135], Zeng et al. used neural network in two ways, pattern recognition and supervised learning. In pattern recognition, data points of nearest neighbor are compared for noise detection; to remove noise, nearest neighbor algorithms are used. In supervised learning, neural network is trained against the data that needs to be captured. Then, neural work is deployed to the actual environment.

5.4 Discussion

The perception layer is responsible for the sensing of the information from the environment. It is a place where the information is gathered and shared with other equipment, as information is the most precious asset of any individual or organization. To ensure the security of the information, several countermeasures are proposed by the researchers. For analysis of the intruder, a formal analytical model is proposed and one must not try to connect with free Internet connections. Secure boot phenomena protect the users from the replication of the firmware code. For information integrity and confidentiality, a scheme termed as a leakage-resilient public-key encryption scheme is proposed. To eradicate noise from the information, the neural network is used in dual formats, one as pattern recognition and the other as supervised learning.

5.5 Physical layer

The physical layer comprises the hardware devices or physical components like, power supplies, smart appliances and smartphones. Power supplies are the backbone of smart home devices. There must be such a mechanism through which these devices can survive during a power interruption. On this layer, devices must be kept safe from the weather. Solutions to such problems are discussed below.

5.5.1 Countermeasure of tag cloning

Kamaludin et al. [58] proposed an accurate and effective method to detect cloned RFID tags in RFID systems. The suggested approach is built on the accuracy of dual hash collisions and a count-min sketch vector. A dual independent hash function is used to map streaming tag reading data. In this system, the combined functionality of dual hash collection and tag reading frequency is carried out to detect duplication of tags.

5.5.2 Network monitoring

Denial of service (DOS) mostly targets network protocol running on the IoT-based smart homes. An intrusion detection system (IDS) plays an important role in detecting, monitoring, and classifying these attacks. IDS also generates alerts to the responsible authorities regarding these attacks.

5.5.3 Secure key management

Usually, network devices are come up with built-in security keys. There should be a comprehensive security key management mechanism to protect smart home devices from intruders to use legitimate devices for their malicious purposes.

5.5.4 Physical protection

Physical devices are usually left unattended, providing a chance for tampering attacks. Physical protection of smart home devices is most important against tampering attacks. Other possible solutions for tampering attacks are reverse engineering and tamper-resistant devices.

5.5.5 Hello flood attack protection

The basic step that can prevent users from hello flood attack is checking of communication link bi-directionally. In [61], Karlof et al. use the identity verification protocol for the verification of the link.

5.5.6 Network-level security

In [110], Sivaraman et al. proposed a solution for the network layer. Network-level security and privacy control is device-level protection augmented with network-level security solutions to detect suspicious behavior of network activity. In this solution, SMP plays a key role in safeguarding the network security.

5.5.7 Security at perception layer

In the TCP/IP network, the most fruitful and successful technique is the public-key infrastructure (PKI). As discussed in Sect. 2, IOT comprises four layers, and each layer needs security relative to that layer. At perception layer security, a new architecture is discussed by Li et al. in [78] called PKI-like protocol. The PKI-like protocol works differently than to PKI protocol in TCP; it works with a short encryption key. In the PKI-like protocol environment, there is a base station and multiple sink points. These sink points are connected to the base station. Short keys are handed out by base stations that act as the public-key center.

5.5.8 Security against DoS

Usually, in the DOS attacks such as jamming or coding, the communication channel is almost useless to perform any communication tasks. Hence, nodes having the IDS installed are unable to perform the detection tasks. Kasinathan et al. in [62] proposed a solution regarding DOS attacks. It can perform the detection activities against the DOS attacks, while not suffering from the same attacks. In a real environment, wireless sensor networks demand an analysis of the physical parameters in real-time. In this regard, service availability is the main need. Consequently, the proposed IDS should detect any kind of DoS activity. The proposed system is evaluated through the PenTest, an evaluation system, and produced expected results against the attacks.

5.6 Discussion

The physical layer consists of hardware components such as power supplies and smartphones. Power is the main source of keeping the network alive. It is necessary to take the ultimate care of such devices. Several techniques and researches are carried out to ensure the safety of such precious components. Count-min sketch vector used a data structure to overcome the problem of tag cloning. Network monitoring is carried out through IDSs. Devices should not be left unattended for intruders. Proper monitoring is necessary for physical devices. Hello flood attack is blocked through identity verification protocol. To encounter real-time intrusions in the IoT network, IDS is proposed.

6 Future directions

In this section, an overview of the future work is discussed in the form of points. In the future, we will extend our study to other security solutions concerning technology and techniques. As IoT is evolving, it consequently faces the most sophisticated issues. So, the mitigation of such issues must be done in a similar fashion.

- Cyber insurance is gaining enlarged consideration these days. From this, more organizations agonize from problems similar to data leakage, data loss, etc. The impairment happens through these proceedings charges extremely to the organizations. So these organizations need to combine defensive intrusion detection and prevention in their structures.
- To detect intrusion and hurriedly implement on the system becomes gradually problematic. So, traditional methods of IDS are not used. The prevention and detection methods are insecurely gathered in Moving Target Defense (MTD). In comparison with NIDS and HIDS, MTD constantly altered the surface of attacks and make the system protected from enemies that enter in the first place.

- In the physical security industry, cloud-centric product development is the greatest noticeable trend. Especially in intrusions field, it is gaining the implementation of cloud-based systems. Superior connectivity and rationalized security operations are some of the well-known benefits which it provides to the users. It is implemented on a cloud-based SaaS model that gives elasticity and flexibility to the machinists. In intrusions field, it is the utmost desire of many manufacturers to get cloud-based solutions.
- Cyber criminals are discovering new ways and techniques for security threats to destruct the system. So in this situation, there is not only necessary to fix the threats as they occur, but also it is essential to learn how to predict and prevent new threats. Modern cloud indicative services are hot topics that are used to predict security concerns intelligently. The AI-powered diagnostic technique is also an interesting field, but it is slightly complex than the former.

7 Conclusion

A smart home is an emerging application of IoT, where devices communicate and share confidential information. In such an environment, several components join hands to complete the objective of IoT, such as smartphones, smart A.C., and smart heater, and sensors like smoke sensors, temperature sensors, etc., and different protocols at the backend. As IoT is new in the market and thus has no security measurements have been done so far by the manufacturer of the devices. Smart devices manufacturers mainly focus on the less computational and low energy consumption devices consequently left behind the security approaches for the devices.

As IOT comprises plethora of devices, when these numerous devices get connected, they face various security and privacy issues. A survey is carried out about the most common security threats and privacy challenges for IoT smart devices. All the issues are categorized according to the layered architecture of the smart home environment. Furthermore, several kinds of literature are surveyed for security solutions and countermeasures against the mentioned challenges. This work gives exposure to the readers about the current and future challenges.

References

1. Abdul-Ghani HA, Konstantas D, Mahyoub M (2018) A comprehensive IoT attacks survey based on a building-blocked reference model. Int J Adv Comput Sci Appl (IJACSA) 9(3):355–373
2. Ahemd MM, Shah MA, Wahid A (2017) IoT security: a layered approach for attacks and defenses. In: 2017 International Conference on Communication Technologies (ComTech), pages 104–110. IEEE
3. Ahlawat B, Sangwan A, Sindhu V. IoT system model, challenges and threats
4. Firoz A, Young-Bae K (2016) Mitigation of black hole attacks in routing protocol for low power and lossy networks. Secur Commun Networks 9(18):5143–5154
5. Ali W, Dustgeer G, Awais M, Shah MA (2017) IoT based smart home: security challenges, security requirements and solutions. In: 2017 23rd International Conference on Automation and Computing (ICAC), pages 1–6. IEEE

6. Farouq A, Tarek S, Shakshuki EM (2018) A detection and prevention technique for man in the middle attack in fog computing. Procedia Comput Sci 141:24–31
7. Alizai ZA, Tareen NF, Jadoon I (2018) Improved IoT device authentication scheme using device capability and digital signatures. In: 2018 International Conference on Applied and Engineering Mathematics (ICAEM), pages 1–5. IEEE
8. Almusaylim ZA, Noor Z (2019) A review on smart home present state and challenges: linked to context-awareness internet of things (IoT). Wirel Networks 25(6):3193–3204
9. Alnaeli SM, Sarnowski M, Aman MS, Abdelgawad A, Yelamarthi K (2016) Vulnerable c/c++ code usage in iot software systems. In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pages 348–352. IEEE
10. Ruth A, Bamidele A, Mohammad H, Jibran S (2020) Internet of things: evolution and technologies from a security perspective. Sustain Cities Soc 54
11. Andrea I, Chrysostomou C, Hadjichristofi G (2015) Internet of things: security vulnerabilities and challenges. In: 2015 IEEE Symposium on Computers and Communication (ISCC), pages 180–187. IEEE
12. Arabo A, Pranggono B (2013) Mobile malware and smart device security: trends, challenges and solutions. In: 2013 19th International Conference on Control Systems and Computer Science, pages 526–531. IEEE
13. Arış A, Oktuğ SF, Berna Örs YS (2015) Internet-of-things security: denial of service attacks. In: 2015 23nd Signal Processing and Communications Applications Conference (SIU), pages 903–906. IEEE
14. Arora A, Kaur A, Bhushan B, Saini H (2019) Security concerns and future trends of internet of things. In: 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), Vol 1, pages 891–896. IEEE
15. Ashibani Y, Mahmoud QH (2018) A behavior profiling model for user authentication in IoT networks based on app usage patterns. In: IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, pages 2841–2846. IEEE
16. Asif W, Ghosh RI, Rajarajan M (2018) An attack tree based risk evaluation approach for the internet of things. In: Proceedings of the 8th International Conference on the Internet of Things, pages 1–8
17. Atlam HF, Wills GB (2020) IoT security, privacy, safety and ethics. In: Digital twin technologies and smart cities, pages 123–149. Springer
18. Azari A, Miao G, Stefanovic C, Popovski P (2018) Latency-energy tradeoff based on channel scheduling and repetitions in nb-IoT systems. In: 2018 IEEE Global Communications Conference (GLOBECOM), pages 1–7. IEEE
19. Bastos D, Shackleton M, El-Moussa F (2018) Internet of things: a survey of technologies and security risks in smart home and city environments
20. Bugeja J, Jacobsson A, Davidsson P (2016) On privacy and security challenges in smart connected homes. In: 2016 European Intelligence and Security Informatics Conference (EISIC), pages 172–175. IEEE
21. Celesti A, Carnevale L, Galletta A, Fazio M, Villari M (2017) A watchdog service making container-based micro-services reliable in iot clouds. In: 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), pages 372–378. IEEE
22. Cesare S (2014) Breaking the security of physical devices. Presentation at Blackhat, 14,
23. Choi J, Jin S (2018) Security threats in connected car environment and proposal of in-vehicle infotainment-based access control mechanism. In: Advanced multimedia and ubiquitous engineering, pages 383–388. Springer
24. Classen J, Chen J, Steinmetzer D, Hollick M, Knightly E (2015) The spy next door: eavesdropping on high throughput visible light communications. In: Proceedings of the 2nd International Workshop on Visible Light Communications Systems, pages 9–14
25. Das D, Maity S, Nasir SB, Ghosh S, Raychowdhury A, Sen S (2017) High efficiency power side-channel attack immunity using noise injection in attenuated signature domain. In: 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pages 62–67. IEEE
26. Datta P, Sharma B (2017) A survey on iot architectures, protocols, security and smart city based applications. In 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pages 1–5. IEEE
27. Denning DE (2012) Stuxnet: What has changed? Futur Internet 4(3):672–687

28. Deogirikar J, Vidhate A (2017) Security attacks in IoT: a survey. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pages 32–37. IEEE
29. Zheng D, Guangzhen S, Yun L, Meiyu W (2019) An adaptive resource allocation model with anti-jamming in IoT network. IEEE Access 7:93250–93258
30. Xiaojiang D, Hsiao-Hwa C, Liehuang Z, Jiangli L, Zheng C (2018) Security and privacy in wireless IoT. IEEE Wirel Commun 25(6):10–11
31. Duangphasuk S, Duangphasuk P, Thammarat C (2020) Review of internet of things (IoT): security issue and solution. In: 2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pages 559–562. IEEE
32. Dhar DA, Gautam S, Shalini D, Rajani S (2019) A decentralized privacy-preserving healthcare blockchain for IoT. Sensors 19(2):326
33. Faisal EM, Ismail AA, Hamed HFA (2018) Intrusion detection systems for IoT-based smart environments: a survey. J Cloud Comput 7(1):21
34. Evans D (2011) The internet of things: how the next evolution of the internet is changing everything. Cisco Int J Internet 3(2):123–132
35. Ezhilarasan E, Dinakaran M (2017) A review on mobile technologies: 3g, 4g and 5g. In: 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), pages 369–373,
36. Fakhri D, Mutijarsa K (2018) Secure IoT communication using blockchain technology. In: 2018 International Symposium on Electronics and Smart Devices (ISESD), pages 1–6. IEEE
37. Pallab G, Mita N, Sourav D (2018) A novel approach for detecting and mitigating the energy theft issues in the smart metering infrastructure. Technol Econ Smart Grids Sustain Energy 3(1):13
38. Gavra V-D, Dobra I-M, Pop OA (2020) A survey on threats and security solutions for IoT. In: 2020 43rd International Spring Seminar on Electronics Technology (ISSE), pages 1–5. IEEE
39. Gendreau AA, Moorman M (2016) Survey of intrusion detection systems towards an end to end secure internet of things. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pages 84–90. IEEE
40. Geneiatakis D, Kounelis I, Neisse R, Nai-Fovino I, Steri G, Baldini G (2017) Security and privacy issues for an iot based smart home. In: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pages 1292–1297. IEEE
41. Ghafir I, Prenosil V, Alhejailan A, Hammoudeh M (2016) Social engineering attack strategies and defence approaches. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pages 145–149. IEEE
42. Ghasemi M, Saadaat M, Ghollasi O (2019) Threats of social engineering attacks against security of internet of things (IoT). In: Fundamental research in electrical engineering, pages 957–968. Springer
43. Gill RK, Sachdeva M (2018) Detection of hello flood attack on leach in wireless sensor networks. In: Next-generation networks, pages 377–387. Springer
44. Gupta Brij B, Arachchilage Nalin AG, Psannis Kostas E (2018) Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst 67(2):247–267
45. Hallman R, Bryan J, Palavicini G, Divita J, Romero-Mariona J (2017) Ioddos-the internet of distributed denial of sevice attacks. In: 2nd International Conference on Internet of Things, Big Data and Security. SCITEPRESS, pages 47–58
46. Hariri Reihaneh H, Fredericks Erik M, Bowers Kate M (2019) Uncertainty in big data analytics: survey, opportunities, and challenges. J Big Data 6(1):44
47. Vikas H, Vinay C, Vikas S, Divyansh J, Pranav G, Biplab S (2019) A survey on IoT security: application areas, security threats, and solution architectures. IEEE Access 7:82721–82743
48. Daojing H, Ran Y, Sammy C, Mohsen G, Yanping X (2018) Privacy in the internet of things for smart healthcare. IEEE Commun Mag 56(4):38–44
49. Mahmud Hossain SM, Riazul I, Farman A, Kyung-Sup K, Ragib H (2018) An internet of things-based health prescription assistant and its security system design. Futur Gener Comput Syst 82:422–439
50. Hossain MM, Fotouhi M, Hasan R (2015) Towards an analysis of security issues, challenges, and open problems in the internet of things. In: 2015 IEEE World Congress on Services, pages 21–28. IEEE
51. Hussain F, Hussain R, Hassan SA, Hossain E (2020) Machine learning in IoT security: current solutions and future challenges. IEEE Commun Surv Tutor

52. Ida IB, Jemai A, Loukil A (2016) A survey on security of IoT in the context of ehealth and clouds. In: 2016 11th International Design and Test Symposium (IDT), pages 25–30. IEEE
53. Islam K, Shen W, Wang X (2012) Security and privacy considerations for wireless sensor networks in smart home environments. In: Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pages 626–633. IEEE
54. ISO/IEC. Iso/iec 27005:2018 (2018). https://www.iso.org/standard/75281.html
55. Kanwal J, Ali SM, Ahmad A, Ali KH, Carsten M, Din IU (2020) Proactive forensics in IoT: privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies. Electron 9(7):1172
56. Jayakumar H, Raha A, Kim Y, Sutar S, Lee WS, Raghunathan V (2016) Energy-efficient system design for IoT devices. In: 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), pages 298–301. IEEE
57. Kalra N, Sharma A, Kumar N, Singh R, Gehlot A (2018) Design and development of IoT-based transmission line monitoring system. In: Intelligent communication, control and devices, pages 465–471. Springer
58. Hazalila K, Hairulnizam M, Abawajy JH (2018) Clone tag detection in distributed rfid systems. PloS one 13(3)
59. Kamel Samah Osama M, Hegazi Nadia H (2018) A proposed model of IoT security management system based on a study of internet of things (IoT) security. Int J Sci Eng Res 9(9):1227–1244
60. Kanuparthi A, Karri R, Addepalli S (2013) Hardware and embedded security in the context of internet of things. In: Proceedings of the 2013 ACM Workshop on Security, Privacy and Dependability for Cyber Vehicles, pages 61–64
61. Karlof C, Wagner D (2003) Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks 1(2–3):293–315
62. Kasinathan P, Costamagna G, Khaleel H, Pastrone C, Spirito MA (2013) An ids framework for internet of things empowered by 6lowpan. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, pages 1337–1340
63. Kaur M, Kalra S (2018) Security in IoT-based smart grid through quantum key distribution. In: Advances in computer and computational sciences, pages 523–530. Springer
64. Khan F, Gawade A Secure data management in smart meter as an application of IoT
65. Hasan AK, Munam AS, Khan S, Ali I, Imran M (2019) Perception layer security in internet of things. Futur Gener Comput Syst 100:144–164
66. Kim D-Y (2014) Cyber security issues imposed on nuclear power plants. Ann Nuclear Energy 65:141–143
67. Kim Y-P, Yoo S, Yoo C (2015) Daot: dynamic and energy-aware authentication for smart home appliances in internet of things. In: 2015 IEEE International Conference on Consumer Electronics (ICCE), pages 196–197. IEEE
68. Ko E, Kim T, Kim H (2018) Management platform of threats information in IoT environment. J Ambient Intell Humanized Comput 9(4):1167–1176
69. Komninos N, Philippou E, Pitsillides A (2014) Survey in smart grid and smart home security: issues, challenges and countermeasures. IEEE Commun Surv Tutor 16(4):1933–1954
70. Konidala DM, Kim D, Chan YY, Lee B (2011) Security framework for rfid-based applications in smart home environment. J Inf Process Syst 7(1):111–120
71. Koo D, Hur J, Yoon H (2013) Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage. Comput Electr Eng 39(1):34–46
72. Kozlov D, Veijalainen J, Ali Y (2012) Security and privacy threats in IoT architectures. In: BODYNETS, pages 256–262
73. Kumar SA, Vealey T, Srivastava H (2016) Security in internet of things: challenges, solutions and future directions. In: 2016 49th Hawaii International Conference on System Sciences (HICSS), pages 5772–5781. IEEE
74. Kumar S, Sahoo S, Mahapatra A, Swain AK, Mahapatra KK (2017) Security enhancements to system on chip devices for iot perception layer. In: 2017 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS), pages 151–156. IEEE
75. Li H, Chen Y, He Z (2012) The survey of rfid attacks and defenses. In: 2012 8th International Conference on Wireless Communications, Networking and Mobile Computing, pages 1–4. IEEE
76. Li S, Da Li X, Zhao S (2015) The internet of things: a survey. Inf Syst Front 17(2):243–259
77. Li X, Wang H, Dai H-N, Wang Y , Zhao Q (2016) An analytical study on eavesdropping attacks in wireless nets of things. Mob Inform Syst

78. Li Z, Yin X, Geng Z, Zhang H, Li P, Sun Y, Zhang H, Li L (2013) Research on pki-like protocol for the internet of things. In: 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation, pages 915–918. IEEE
79. Lin H, Bergmann NW (2016) IoT privacy and security challenges for smart home environments. Information 7(3):44
80. Liu J, Xiao Y, Chen CLP (2012) Authentication and access control in the internet of things. In: 2012 32nd International Conference on Distributed Computing Systems Workshops, pages 588–592. IEEE
81. Liu Y, Briones J, Zhou R, Magotra N (2017) Study of secure boot with a fpga-based IoT device. In: 2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS), pages 1053–1056. IEEE
82. Maurer U (2011) Constructive cryptography—a new paradigm for security definitions and proofs. In: Joint Workshop on Theory of Security and Applications, pages 33–56. Springer
83. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A (2019) IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Int Things J 6(5):8182–8201
84. Shunmei M, Zijian G, Qianmu L, Hao W, Hong-Ning D, Lianyong Q (2020) Security-driven hybrid collaborative recommendation method for cloud-based IoT services. Comput Secur 97
85. Miorandi D, Sicari S, De Pellegrini F, Chlamtac I (2012) Internet of things: Vision, applications and research challenges. Ad Hoc Networks 10(7):1497–1516
86. Mosenia A, Jha Niraj K (2016) A comprehensive study of security of internet-of-things. IEEE Trans Emerg Top Comput 5(4):586–602
87. Mujica G, Portilla J (2019) Distributed reprogramming on the edge: a new collaborative code dissemination strategy for IoT. Electronics 8(3):267
88. Muthukrishnan H, Sunita B, Najeerabanu S, Yasuvanth V (2020) Observational study of wpan and lpwa technologies for various IoT devices and its applications
89. Nirmal K, Janet B, Kumar R (2020) Analyzing and eliminating phishing threats in IoT, network and other web applications using iterative intersection. Peer-to-Peer Network Appl, pages 1–13,
90. Perrig A, Stankovic J, Wagner D (2004) Security in wireless sensor networks. Commun ACM 47(6):53–57
91. Perwej Y, Omer MK, Sheta OE, Harb HAM, Adrees MS (2019) The future of internet of things (iot) and its empowering technology. Int J Eng Sci, 20192
92. Pongle P, Chavan G (2015) A survey: attacks on rpl and 6lowpan in IoT. In: 2015 International Conference on Pervasive Computing (ICPC), pages 1–6. IEEE
93. Porkodi R, Bhuvaneswari V (2014) The internet of things (IoT) applications and communication enabling technology standards: an overview. In: 2014 International Conference on Intelligent Computing Applications, pages 324–329. IEEE
94. Prokofiev AO, Smirnova YS, Surov VA (2018) A method to detect internet of things botnets. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pages 105–108. IEEE
95. Ramesh G, Krishnamurthi I, Sampath Sree Kumar K (2014) An efficacious method for detecting phishing webpages through target domain identification. Decis Support Syst 61:12–22
96. Tariq AR, Haq EU (2018) Security challenges facing iot layers and its protective measures. Int J Comput Appl 975:8887
97. Rizvi S, Kurtz A, Pfeffer J, Rizvi M (2018) Securing the internet of things (IoT): a security taxonomy for IoT. In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pages 163–168. IEEE
98. Roberts CM (2006) Radio frequency identification (rfid). Comput Sec 25(1):18–26
99. Robles RJ, Kim T, Cook D, Das S (2010) A review on security in smart home development. Int J Adv Sci Technol 15
100. Rodrigues Luis, Guerreiro Joel, Correia Noélia (2020) Reload/coap architecture for the federation of wireless sensor networks. Peer-to-Peer Networking and Applications 13(1):27–37
101. Said O, Albagory Y, Nofal M, Fahad AR (2017) Iot-rtp and IoT-rtcp: adaptive protocols for multimedia transmission over internet of things environments. IEEE access 5:16757–16773
102. Salman O, Elhajj I, Chehab A, Kayssi A (2018) Iot survey: an sdn and fog computing perspective. Comput Networks 143:221–246

103. Sarkar AR, Sanyal G, Majumder S (2016) Application of wireless technology for a vision based rehabilitation system. In: 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pages 106–111. IEEE
104. Savola RM, Abie H, Sihvonen M (2012) Towards metrics-driven adaptive security management in e-health iot applications. In BodyNets, pages 276–281
105. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. J Electr Comput Eng
106. Shamsoshoara A, Korenda A, Afghah F, Zeadally S (2019) A survey on hardware-based security mechanisms for internet of things. arXiv preprint arXiv:1907.12525
107. Sharma P, Zawar S, Patil Suryakant B (2016) Ransomware analysis: internet of things (IoT) security issues challenges and open problems inthe context of worldwide scenario of security of systems and malware attacks. Int Conf Recent Innov Eng Manag 2:177–184
108. Siddiqui ST, Alam S, Ahmad R, Shuaib M (2020) Security threats, attacks, and possible countermeasures in internet of things. In: Advances in data and information sciences, pages 35–46. Springer
109. Silva I, Leandro R, Macedo D, Luiz AG (2013) A dependability evaluation tool for the internet of things. Comput Electr Eng 39(7):2005–2018
110. Sivaraman V, Gharakheili HH, Vishwanath A, Boreli R, Mehani O (2015) Network-level security and privacy control for smart-home IoT devices. In: 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pages 163–167. IEEE
111. Sonar K, Upadhyay H (2014) A survey: Ddos attack on internet of things. Int J Eng Res Dev 10(11):58–63
112. Suo H, Wan J, Zou C, Liu J (2012) Security in the internet of things: a review. In: 2012 International Conference on Computer Science and Electronics Engineering, Vol. 3, pages 648–651. IEEE
113. Swamy SN, Jadhav D, Kulkarni N (2017) Security threats in the application layer in IoT applications. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pages 477–480. IEEE
114. Tang X, Ren P, Han Z (2018) Jamming mitigation via hierarchical security game for IoT communications. IEEE Access 6:5766–5779
115. Thangavel C, Sudhaman P (2017) Security challenges in the IoT paradigm for enterprise information systems. In: Connected environments for the internet of things, pages 3–17. Springer
116. Varga P, Plosz S, Soos G, Hegedus C (2017) Security threats and issues in automation IoT. In: 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), pages 1–6. IEEE
117. Vashi S, Ram J, Modi J, Verma S, Prakash C (2017) Internet of things (IoT): a vision, architectural elements, and security issues. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pages 492–496. IEEE
118. Venkata Abhishek N, Tandon A, Lim TJ, Sikdar B (2018) Detecting forwarding misbehavior in clustered iot networks. In: Proceedings of the 14th ACM International Symposium on QoS and Security for Wireless and Mobile Networks, pages 1–6
119. Vimal Jerald A, Rabara SA, Bai TDP (2015) Internet of things (IoT) based smart environment integrating various business applications. Int J Comput Appl 128(8):32–37
120. von Tschirschnitz M, Peuckert L, Franzen F, Grossklags J (2020) Method confusion attack on bluetooth pairing. Under submission
121. Vuppala S, Alie El-Din M, Kuenzi A (2019) Moving target defense mechanism for side-channel attacks. IEEE Syst J 14(2):1810–1819
122. Wallrabenstein JR (2016) Practical and secure IoT device authentication using physical unclonable functions. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pages 99–106. IEEE
123. Wang P, Chaudhry S, Li L, Li S, Tryfonas T, Li H (2016) The internet of things: a security point of view. Internet Res
124. Wang Z (2019) Identity-based verifiable aggregator oblivious encryption and its applications in smart grids. IEEE Trans Sustain Comput
125. Wei D, Qiu X (2018) Status-based detection of malicious code in internet of things (IoT) devices. In: 2018 IEEE Conference on Communications and Network Security (CNS), pages 1–7. IEEE
126. Werbach K, Mehta A (2014) The spectrum opportunity: sharing as the solution to the wireless crunch. Int J Commun 8:22

127. Werner M, Unterluggauer T, Schaffenrath D, Mangard S (2018) Sponge-based control-flow protection for IoT devices. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pages 214–226. IEEE
128. Whittaker C, Ryner B, Nazif M (2010) Large-scale automatic classification of phishing pages
129. Winter T, Thubert P, Brandt A, Hui JW, Kelsey R, Levis P, Pister K, Struik R, Vasseur J-P, Alexander RK, et al (2012) Rpl: Ipv6 routing protocol for low-power and lossy networks. rfc, 6550:1–157
130. Wu M, Lu T-J, Ling F-Y, Sun J, Du H-Y (2010) Research on the architecture of internet of things. In: 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), Vol 5, pages V5–484. IEEE
131. Xiang G, Hong J, Rose CP, Cranor L (2011) Cantina+ a feature-rich machine learning framework for detecting phishing web sites. ACM Trans Inform Syst Secur (TISSEC) 14(2):1–28
132. Xiaohui X (2013) Study on security problems and key technologies of the internet of things. In: 2013 International Conference on Computational and Information Sciences, pages 407–410. IEEE
133. Yoon S, Park H, Yoo HS (2015) Security issues on smarthome in IoT environment. In: Computer science and its applications, pages 691–696. Springer
134. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC (2017) A survey of intrusion detection in internet of things. J Network Comput Appl84:25–37
135. Zeng X, Martinez T (2003) A noise filtering method using neural networks. In: IEEE International Workshop on Soft Computing Techniques in Instrumentation, Measurement and Related Applications, 2003. SCIMA 2003 pages 26–31. IEEE
136. Zhang T, Antunes H, Aggarwal S (2014) Defending connected vehicles against malware: Challenges and a solution framework. IEEE Internet Things J 1(1):10–21
137. Zhao W, Yang S, Luo X (2020) On threat analysis of IoT-based systems: a survey. In: 2020 IEEE International Conference on Smart Internet of Things (SmartIoT), pages 205–212. IEEE

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Haseeb Touqeer[1] · Shakir Zaman[1] · Rashid Amin[1] · Mudassar Hussain[2] · Fadi Al-Turjman[3] · Muhammad Bilal[4]

Haseeb Touqeer
ht.alizai@gmail.com

Shakir Zaman
muhammadshakir93@gmail.com

Mudassar Hussain
mhtarar@gmail.com

Fadi Al-Turjman
fadi.alturjman@neu.edu.tr

[1] Department of Computer Science, University of Engineering and Technology, Taxila, Pakistan

[2] Department of Computer Science, University of Wah, Wah Cantt, Pakistan

[3] Department of Artificial Intelligence Engineering, Research center for AI and IoT, Near East University, Mersin 10, Nicosia, Turkey

[4] Department of Computer Engineering, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 17035, Korea