IEEE Open Journal of
Vehicular Technology

Received 27 December 2022; accepted 29 December 2022. Date of publication 4 January 2023;
date of current version 14 February 2023. The review of this article was coordinated by Editor Lina Mohjazi.

Digital Object Identifier 10.1109/OJVT.2023.3234069

Cyber-Security of Embedded IoTs in Smart Homes: Challenges, Requirements, Countermeasures, and Trends

AAESHA ALDAHMANI, BASSEM OUNI (Member, IEEE), THIERRY LESTABLE,
AND MEROUANE DEBBAH (Fellow, IEEE)

(Invited Paper)

Technology Innovation Institute, 9639 Masdar, UAE

CORRESPONDING AUTHOR: BASSEM OUNI (e-mail: bassem.ouni@tii.ae)

This work was supported by the Technology Innovation Institute, Abu Dhabi, UAE.

ABSTRACT Connected computers and sensors transmit data across the Internet to solve problems and generate new services (IoT). Smart homes use IoT, for example. Smart home technology can monitor temperature, detect smoke, regulate lighting automatically, and install smart locks. It also poses additional security and privacy problems, such as accessing user data through surveillance equipment or false fire alarms. Smart homes are vulnerable to numerous sorts of assaults. This survey emphasizes IoT. We discuss IoT's design, objects, and standards. We also address the tiered Internet of Things framework and smart home security concerns. In this article, researchers examine IoT-based smart home difficulties and offer solutions.

INDEX TERMS IoT devices, smart homes, Cyber-security, architecture, attacks, embedded systems.

I. INTRODUCTION

The Internet of Things (IoT) is defined as "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face situations and changes in the environment" [1]. IoT is a cutting-edge technology that is changing the way we live. An autonomous smart home is equipped with embedded devices that are designed to detect and respond to a person's presence and needs such as light detection devices, fingerprint readers, gas detection systems, smoke sensors, temperature monitoring devices, motion detection systems, home surveillance cameras, etc. These devices are connected together for many purposes such as saving energy consumption, reducing the bill costs, and security of home occupants [2]. Users are using interface devices such as a remote control, computer, or smartphone to manipulate different sensors and devices in these systems [3].

Nowadays, the use of IoT-enabled smart home systems is significantly growing around the world to allow residents to live more comfortably, easily, and smoothly [4], [5]. According to IoT Analytics' latest reports "In 2021, IoT Analytics expects the global number of connected IoT devices to grow by 9% to reach 12.3 billion active endpoints. By 2025, there will likely be more than 27 billion IoT connections [6]. With this huge increase in the number of connected devices, the spectrum of attack surface increases accordingly, and any security flaws can represent the weakest link thus becoming an attack entry point. Moreover, these devices communicate directly, or indirectly, with each other using several protocols such as Bluetooth, Wi-Fi, Zigbee etc and they are connected to the home internet service. Securing such communications, devices and applications becomes in the past few years an increasingly complex and leading-edge challenge for IoT network designers [7].

A smart home comprises all the interconnected sensors and appliances and is monitored through one central monitoring end-point, which can be a smartphone, tablet, computer etc. The "things" that can be controlled are doors, locks, air conditioners, devices, thermostats, screens, lights, cameras, and refrigerators. Fig. 2 shows the communications between smart home devices. Frequently, smart home devices are connected online and can be controlled remotely, for instance, using a

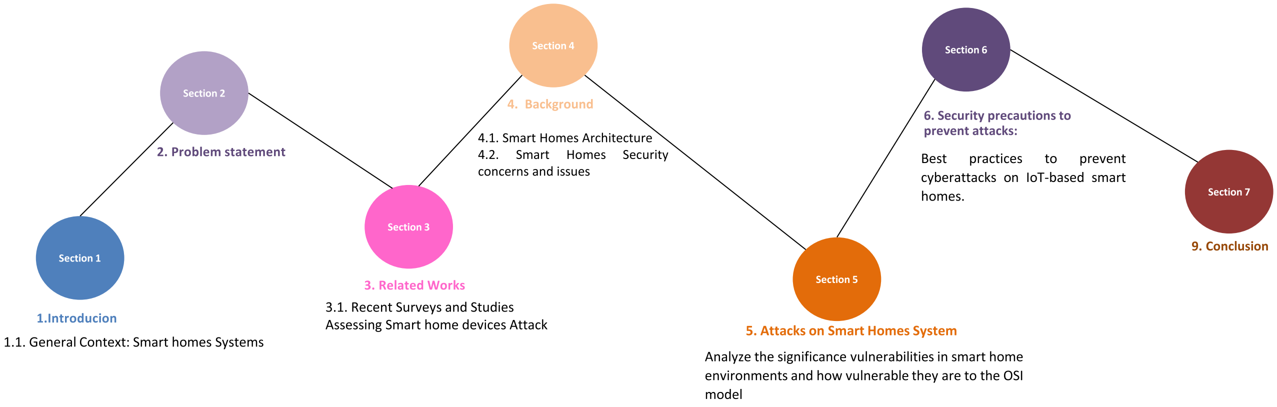
Section 1
1.Introducion
1.1. General Context: Smart homes Systems
Section 2
2. Problem statement
Section 3
3. Related Works
3.1. Recent Surveys and Studies Assessing Smart home devices Attack
Section 4
4. Background
4.1. Smart Homes Architecture
4.2. Smart Homes Security concerns and issues
Section 5
5. Attacks on Smart Homes System
Analyze the significance vulnerabilities in smart home environments and how vulnerable they are to the OSI model
Section 6
6. Security precautions to prevent attacks:
Best practices to prevent cyberattacks on IoT-based smart homes.
Section 7
9. Conclusion

FIGURE 1. Organization of the review paper.

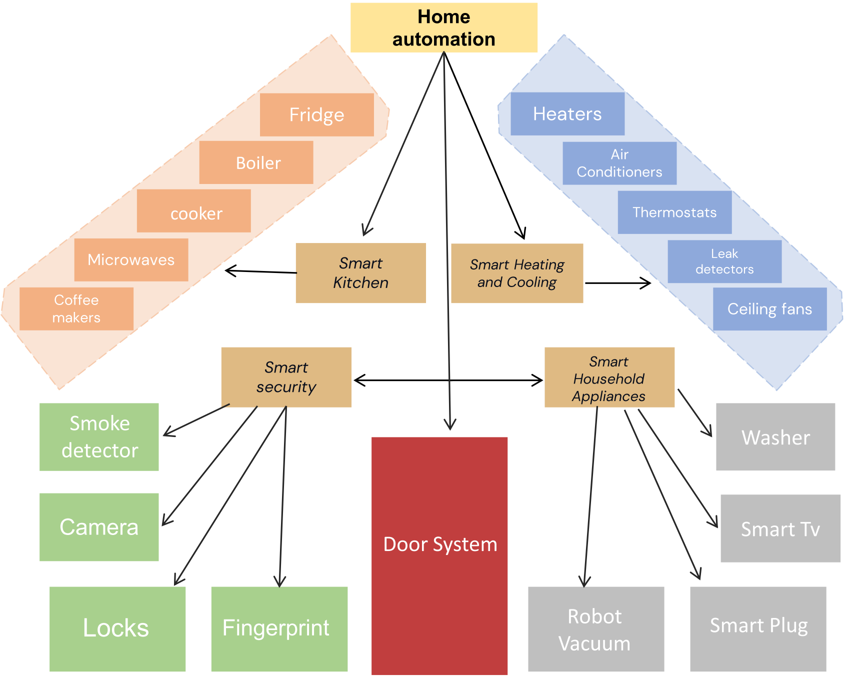

FIGURE 2. Smart home devices communications.

cloud and/or mobile application. This is extremely convenient for the user and can reduce costs thanks to the scalability of usage, but it can also introduce problems [8]. Typically, users may control and manage the security of these devices using a desktop or mobile application. Users are fearful of hackers who can gain access to private and confidential data such as Health monitoring systems, but also credit card numbers for automatic retailing orders, causing damages by running Air conditioning, and decreasing the temperature of fridges.

The rest of the paper is organized as follows. In Section II, we will discuss the problem of cyber-security in smart homes. The recent surveys and studies assessing smart home device attacks are addressed in Section III. Smart home architecture is introduced in Section IV and the security issues are discussed in more detail in Section V. The next Section VI addresses the precautions to prevent these attacks in different layers. Finally, conclusions and perspectives are highlighted in Section VII. Fig. 1 shows the layout of the survey.

II. PROBLEM STATEMENT

The internet has grown a lot during the past few decades and has become a necessity. Berners-Lee played a significant role in the development of the internet and shaping the World Wide Web. According to Berners-Lee, the Internet of Things (IoT) must be open, free, and available to everyone (IoT). With 24 billion devices expected to be online in the public domain by 2025, several security vulnerabilities can lead to a variety of serious problems if they are not properly protected or configured. Different personal information is collected by a variety of connected devices such as name, date of birth, address, credit card information, etc. several millions of dollars, and could impact the customer-company relationship in terms of customer trust and brand value [9], [10]. Ransoms are rising, in 2021, about 11% of companies and businesses in the US paid 1 million dollars. Hackers are not making it cheap, the number of companies paying less than 10,000 dollars was at 34% but decreased to 21%.

Several threats result in the unwanted release of sensitive information. For instance, a confidential breach in a smart home system can result in the release of the sensitive medical data of a certain house. Several threats also include unauthorized access to a system controller at an administrator level, which makes the entire system insecure [11]. Moreover, these connected devices have several attack surfaces and could have several vulnerabilities. Many attacks can be carried out remotely, either by direct access to the control interface or by installing malware in the system.

This paper focuses on the main serious cyber-security challenges of IoT devices used in smart connected homes. We will introduce a taxonomy related to vulnerabilities, threats and attacks on IoT devices. Moreover, we will highlight several recommended and countermeasures security solutions that can be used to keep IoT devices, networks, and applications cyber-safe and protect them against cyberattacks. The following are the work's innovation keys:

1) expanding a study architecture and smart home system attacks.
2) We address various attacks that we classify in three different layers of the system.
3) We cover attacks on the sensor and other devices in smart homes.

Since this work focuses on specifically embedded IoT security issues, the key research questions we are addressing are as follows:

- (Q1): What is the architecture of a smart home?
- (Q2): What are the main smart home system vulnerabilities and security concerns?
- (Q3): Which are the attacks on the perception layer (sensors)?
- (Q4): Which are the attacks that target communication and Network?
- (Q5): What are the defensive measures against device attacks in a smart home (sensors, appliances, or actuators)?
- (Q6): What are the defensive measures against software application attacks of modern smart homes (end devices and gateways)?
- (Q7): What are the future research directions and the open perspectives for securing Smart Home systems?

III. RELATED WORKS

Several research works target to exploit of security flaws in IoT devices in order to comprehend the disease, bring a suitable solution used in the Internet of Things and the Smart Home environments that will promptly detect its symptoms (IDS), treat it, and then protect it. A cyber-attack aims to change, destroy, intercept, manipulate, or steal data. Moreover, it could exploit or harm a network. These works target to implement several methodologies and develop tools to protect against malicious threats being able to control smart home devices and steal information from them. Smart home devices have several vulnerabilities and are exposed to different attacks, such as Man-in-the-middle, Data Breach, Identity theft, Device hijacking, Spoofing and Distributed Denial of Service (DDoS). These attacks are classified into three types of security properties: availability, integrity, and confidentiality. In this section, we will go over several recent articles about smart home security concerns.

The authors in [12] proposed a four-layered cybersecurity-oriented architecture dedicated to the IoT devices and describe each layer of it, such as sensing, networking, middleware and application. Moreover, the authors identify the attack type targeting each layer. In addition, they categorize different attacks into eight classifications which are device, location, access level, information damage level, host promise, strategy, protocol-based, layer-based, and major attacks. The authors summarized the different IoT architectures from a security perspective and introduced different research challenges and future trends.

The authors in [12] proposed a four-layered cybersecurity-oriented architecture dedicated to the IoT devices and describe each layer of it, such as sensing, networking, middleware and application. Moreover, the authors identify the attack type targeting each layer. In addition, they explored the IoT security main countermeasures from a layer-level perspective. The authors summarized the key application in industries and introduced different research challenges and future trends.

Ali et al. [13], presented OCTAVE Allegro, a new method that focuses mainly on information assets to identify security threats and the potential risks in an IoT-based smart home environment. Moreover, they describe the consequences and potential impacts of these risks and defined risk scores for such purposes. As a perspective, they were looking to create a framework to identify and assess security risks in IoT-based smart homes.

In [14], Saxena et al. described the types of attacks in smart home networks and categorized them into two groups: passive and active attacks. In addition, the authors refined Distributed Denial of Service Attack Types, and they listed several tools that are used either internally or externally in Smart Home Networks. The experimental setup in this work focused on the identification and mitigation DDoS by using Wireshark to extract the network traffic as input data. That data includes Attack duration, Response Time, Server downtime, Port used, Protocol used, DNS type and Packet Length. After extracting features, they generate a Graph based on the attack threshold and identify the choking node. Finally, they apply the shortest path algorithm to mitigate DDoS attacks.

Abdullah et al. [15] showed that popular vulnerabilities are primarily resulting from only 6 flaws, outdated protocols, weak encryption, limited storage and CPU, insecure applications, poor authentication, and firmware failure. In terms of threats, they showed 4 or 5 main threats categories of threats only such as denial of Service (DoS), eavesdropping, impersonation, compromising and Malicious Software in smart home networks. This paper presented the best user practices and recommended security solutions for smart home environments like updating the software, changing credentials regularly and monitoring the network.

In [16], the authors present the major vulnerabilities of smart home devices. They divide the attacks into four main groups which are physical, network, software, and encryption. Also, determine whether any vulnerabilities of any kind had been discovered in the specific IoT devices. The first vulnerability analysis is between two different devices but further proof is required. As a result, they examine four products from the same utility category, smart lighting. The majority of vulnerability analyses focus on well-known products and vendors. According to their experiments, well-known vendor and devices have greater security postures than less well-known devices.

In the remaining of this paper, we present the architecture of a smart home system. Then, we highlight its different vulnerabilities and security concerns at different levels of abstraction: application, transport, network, and perception levels. After that, we addressed research directions and open perspectives for securing smart home systems.

IV. BACKGROUND: SMART HOME ARCHITECTURE AND SECURITY ISSUES

A. SMART HOME ARCHITECTURE

In recent decades, smart homes have evolved into residences that enable Internet-connected devices to control and monitor household equipment and systems. The Internet of Things (IoT) refers to these gadgets, which are outfitted with sensors, actuators, software, and data processing capabilities. Smart home gadgets were initially employed as a type of remote on/off switch, but have since grown into devices that can govern our homes based on established patterns and scenarios or the user's preferences. The architecture of the IoT Smart Home is divided into many layers such as perception, transport, network and applications [17], [18]. These layers should not be considered distinct and unrelated to each other, but complement each other [17] and aim to provide a service, access, connection and control of things via the Internet at any time and from any location. The perception layer of the smart home environment focuses on the physical component that contains hardware devices. The sensor is one of the physical resources that can monitor the environment sensing as motion, light, door and temperature, hence collecting the information and transmitting it to the devices through a network [18]. The transmission process should be carried out by the transport layer [19]. each another [17] and aim to provide a service, access, and control of things via the Internet at any time and from any location. The perception layer of the smart home environment focuses on the physical component that contains hardware devices/ sensors and actuators. Sensors are one of the physical resources that can capture information from real-world environments like motion, light, door and temperature, hence collecting the information and transmitting it to the devices through a network [18]. The transmission process should be carried out by the transport layer [19].

The application layer will hold devices either to dashboard received data from devices or to monitor them remotely. The network layer is responsible for transferring collected data to the processing unit or application [20].

A sample of smart home system architecture with different layers is depicted in Fig. 3.

The data is transmitted across the network as follows:

The data is wirelessly transmitted from end devices to a cloud platform via LPWAN (low power wide area network). MQTT and HTTP are the two protocols that Cloud IoT Core supports for efficient data transport. Using either the MQTT bridge or the HTTP bridge, devices connect to Cloud IoT Core. In addition, the gathered data from the wireless sensor network will be uploaded to cloud storage through gateways. Following the acquisition, the data is stored in the cloud and will be accessible to users there. A back-end application, storage devices, and a front-end application shape the Cloud solution. In the back end, the data is processed and analyzed using specific cloud engines (such as Google App Engine) or in-premises workstations. Once the application layer is established, the user can visualize the environment, and manage services and devices using a web or mobile application [18]. The user interface connects the user with smart devices. The commands could monitor these devices in several ways, notably the voice. Due to its ease of use, the voice user interface (VUI) has recently become the most popular [19]. There are many intelligent voice control devices such as Alexa, Google Home, Apple Siri Amazon Echo that use NLP (natural language processing) machine learning technology, which transfers human speech into a written format and replies to the user's request.

Furthermore, the communication gap between end devices, sensors, systems, and the cloud is bridged and secured by a gateway device [17]. The gateway is used efficiently to remotely control home devices, and monitor, and authenticate communication between IoT devices in the system. The mobile device might control either gateway or devices at the perception layer [21]. Accordingly, data is routed through the gateway from the sender to the recipient. The IoT has enough computing power to process data at the network's edge before transmitting it to the cloud [15]. Moreover, the gateway adds a layer of security to the smart home network because it connects end devices to the external network, allowing all communication to be filtered before commands reach the end devices [18].

B. SMART HOMES SECURITY CONCERNS AND ISSUES

Technology and innovation trends have motivated people to adapt to a comfortable lifestyle carried out by smart home devices. Although smart home devices are convenient to use and relate several advantages for security and safety concerns, they are prone to Cybersecurity risks [22], [23] Indeed, due to people's negligence and several device vulnerabilities, various cases provide evidence that intelligent home automation has

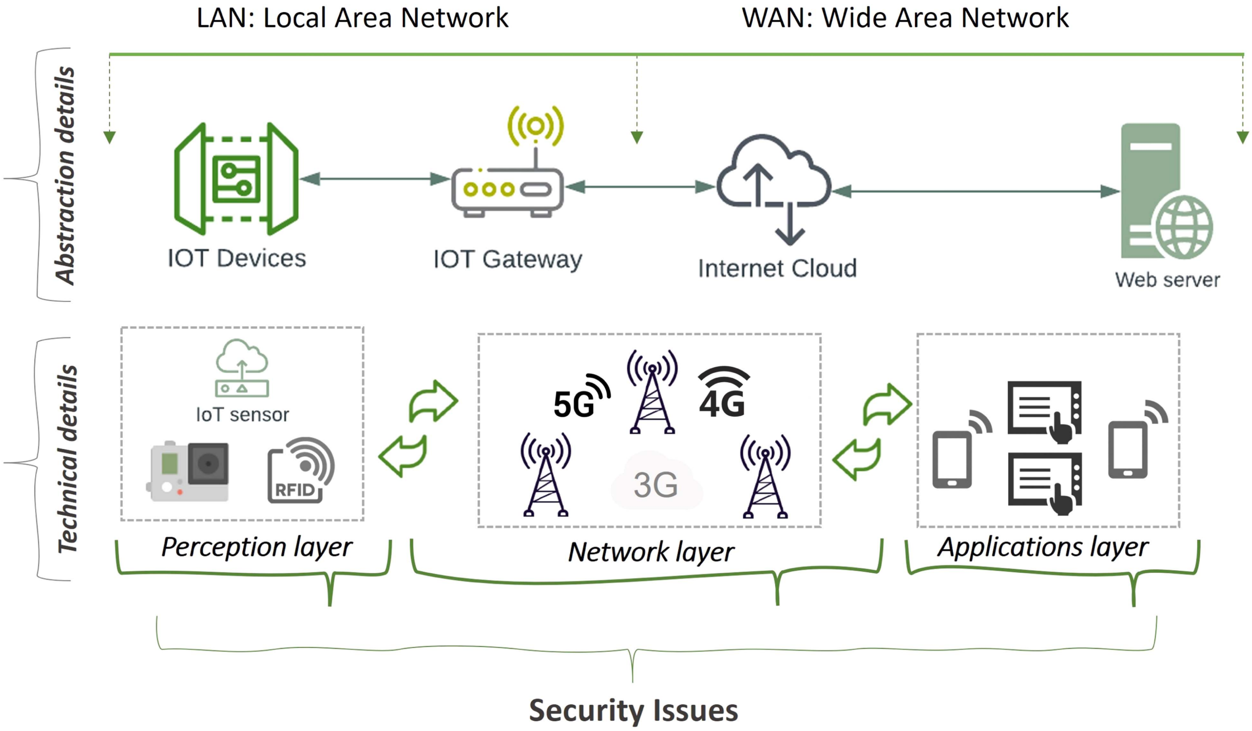

FIGURE 3. Architecture of IoT system.

been hacked on multiple occasions [24]. This raises the risk of concern for Cybersecurity among individuals that greatly rely on smart home automation. It is essential for individuals also to stay concerned about their safety and security processes, mainly towards the relevance of smart home automation [25]. Better assessment of the Cybersecurity framework, analysis of the threat areas, and better evaluation of the network-based processes need to be processed. Due to the lack of clear user guidance, the poor in-built security measures can be easily hacked, leading to the infiltration of hackers into the security system, and accessing the whole network from the smart home automation system [26]. With respect to the concept of physical attacks targeting smart home devices, it is essential to note that there is a likeliness of vulnerabilities affecting the security of the smart devices [23]. Smart homes are also prone to physical attacks, by tampering with digital wires and installing low-quality sensors. Moreover, while the engagement of the external processes might not be seen as dangerous, the real danger is processed after firing up the gadgets. These issues with physical attacks affect the data integrity due to a lack of control and evidence entertained in the security of the hardware and software systems of the devices [26].

V. ATTACKS ON SMART HOMES SYSTEMS

The rise of smart homes has an impact on many aspects of a user's life. A variety of sensors, including cameras, microphones, motion detectors, and activity loggers, will keep an eye on them. While these smart homes offer convenient features like voice-activated lighting and remote-controlled door locks, the Risks to privacy and security associated with internet-connected devices in homes have been brought up by security experts. Insecure communication leaking private information about the home and its occupants, and device vulnerabilities that could be exploited by an attacker to spy on or otherwise interfere with the residents' lives remotely are among the issues raised. [27] All these systems are intended to provide useful services for a better quality of life; however, data leakage raises privacy concerns. To create a smart home, four layers of connected automation systems must be considered:

- Transport layer
- Perception layer
- Application layer
- Network layer

Table 1 shows the IoT devices in each layer and the attacks in smart home systems.

- **Transport layer:**

MQTT is designed for IoT and M2M message transfer; data is transferred over TCP. MQTT uses IP/TCP and leverages Transport Layer Security to ensure the whole connection is encrypted. MQTT is important in event-based data or streaming data. Many IoT applications use MQTT because it can be used in constrained applications and sending payload. Another protocol, named CoAP, relies on UDP security features to protect information. As HTTP uses TLS over TCP, CoAP uses Datagram TLS over UDP. The following attacks can be exploited in the transport layer:

TABLE 1. **Smart Home Attacks at Different Levels of Layers**

Layer	IoT device/Application	Purpose	Attack object
Perception	Physical objects, Sensors, Actuators	Collect information from sensors/devices	Physical damage, Eavesdropping, Node capture, Replay attack, Timing attack
Network/Transport	Router, Gateways, LoraWAN, 3G, 4G	Connect devices to each other and higher layer through wired/wireless media	Full control, Eavesdropping, Traffic analysis, DoS Attack, Man in the middle, DDoS
Application	Household appliances	Has the responsibility to extend sensor-specific service to application/clients	Take control, To identify speakers, Cross-site scripting, Malicious canr overflow

1) Replay attack: in a replay attack, a third party eavesdrops on communications between two trustworthy parties and then relays them as if they were coming from them. The attacker has the ability to copy and store a legitimate service request issued from a device connected to the smart home network. Play it again later to access the service that a home user is allowed to utilize.
2) Message modification: Messages may be altered when outsiders attempt to intercept conversations between authorized parties, modify the software to perform maliciously or change the values of information.
3) DOS: denying services Attacks are used when a hacker wishes to deny access to a network to legitimate users or restrict the availability of network services. The attacker can broadcast an endless stream of messages to deplete the smart home network system's resources. As a result, authorized users cannot access the services provided by the home network. By flooding servers and other Internet-connected devices with messages, the intrusion can also restrict internal traffic sent through wired or wireless networks inside the smart home.

- **Perception layer:**

It is often referred to as the sensor layer. It operates similarly to the human eyes, hearing, and nose. It is responsible for identifying objects and extracting information from them. Several types of information-collecting sensors include RFID, 2-D barcode, and sensors. The sensors are selected based on the requirements of the applications. MEMS is one of these sensors that detect changes in their surroundings and monitor physical or environmental conditions in homes. Moreover, rotational motion is measured using gyroscopes. So, it can detect When a door or window is opened and closed. By observing their mobility, the position sensor can determine whether there are people or other objects in a certain space. Thanks to these sensors, the owner may track the doors and windows of rooms and appliances from anywhere for home security. The information collected by these sensors may pertain to position, air quality, surroundings, motion, vibration, etc. However, they are the primary target of attackers seeking for spoofing or jamming these sensors. Consequently, the majority of threats at this level concern the sensors. Common perception layer security concerns are:

1) Eavesdropping: is a type of illegal real-time attack in which an attacker intercepts private communications like phone calls, text messages, fax transmissions, or video conferences. It tries to steal data transmitted via a network. Then, it takes advantage of insecure communication to gain access to both transmitted and received data. Furthermore, previous works, for example, the one relevant to the Dolphin attack in [28], have shown that attackers can hide their voice commands by modulating them on ultrasonic carriers and use inaudible voice attacks to manipulate mobile devices. The authors in [28] tested their attack against Siri, Google Now, Samsung S Voice, Huawei HiVoice, Cortana, and Alexa, among other popular speech recognition systems
2) Node Capture: one of the significant attacks faced in the perception layer that can be used against wireless sensor networks. It allows an attacker to simply compromise the entire network and it has the potential to reveal all important security information including sender-receiver conversations, shared secrets and cryptography keys.
3) Replay Attack: A replay attack, also known as an interceptor attack. An intruder listens to the sender-recipient communication and steals authentic information from the sender [29]. An intruder gives the victim the same confirmed information that the victim has previously received by presenting evidence of his identity and authenticity. The message is encoded so that the recipient can interpret it as a valid request and carry out the intruder's intent.
4) Timing Attacks: are most commonly used against devices with limited processing capabilities. An attacker can identify weaknesses and steal secrets stored in a system's by observing the time it takes for a system to respond to various requests, input, or cryptography methods.

- **Application Layer**:

Application layer protocols are crucial in a heterogeneous IoT environment. They define the communications between IoT devices and the network. These devices could be monitored and controlled through several applications in a smart home environment. A system weakness at the application level could be exploited to compromise the security of the whole IoT network and access to personal and private data relevant. Common application layer security challenges and problems include:

1) Cross-Site Scripting: is a form of injection attack and known as Web attack. These types of attacks are not difficult to detect and recognize, but they are challenging to differentiate from and defend against. It typically targets the applications running on the user side rather than the server side. [30]. It happens when malicious web code, typically in script form, is delivered or executed from the victim's computer's browser via certain web applications. An attacker might then find personal information or steal the user's cookies to hijack. Moreover, allow the attackers the opportunity to acquire sensitive information or even gain control over specific devices [31].
2) Malicious Code Attack: related to any software code that is intended to harm the system. An attacker can utilize an end-user attack to get access to a system and inject any type of malicious code inside in order to steal data from users [32]. It is a type of threat that may not be blocked or controlled by the use of anti-virus tools.
3) Buffer overflow: IoT devices are now vulnerable to numerous software and hardware vulnerabilities, including buffer overflow attacks. A buffer serves as a temporary storage location for data in a buffer overflow attack, which occurs when the storage space is exceeded [33]. In [34], the authors present a buffer overflow attack detection hardware design with architectural enhancements.

- **Networking layer:**

Smart home devices use network layer protocols such as Bluetooth, IrDA, WiFi, ZigBee, RFID, NUWB, NFC, Wireless Hart, and other communication technologies to connect devices, networks, and servers. Attackers are most likely to target wireless networks at the network layer. The main risks in network communication are relevant to poor confidentiality settings and authentication. Moreover, Malicious actors use insecure networks to launch network eavesdropping attacks, also known as network sniffing or network snooping attacks. Several examples of attacks include:

1) DoS Attack: A DoS attack is an attempt to block access to devices or other network resources by actual users. The majority of the time, this is accomplished by overloading the targeted devices or network resources with requests, making it difficult or impossible for some or all actual users to use them.
2) Man-in-the-middle (MiTM) assault: In a man-in-the-middle (MiTM) attack, the attacker secretly listens and modifies the dialogue between the sender and the recipient, who both believe they are speaking to each other directly. Being in control of communication allows the attacker to alter the messages to suit their purposes. Because it allows the attacker the capacity to obtain information and alter it in real time, it poses a serious threat to internet security. A group of hackers recently identified a man-in-the-middle flaw in a Samsung smart refrigerator. It was discovered by hackers that the device does not check SSL certificates, giving them access to the network and the ability to obtain the login information of Gmail users and keep track of activities for the username and password needed to connect the refrigerator to Gmail.
3) DDoS: One of the most significant dangers to the Internet is distributed denial-of-service or DDoS. There are two mechanisms commonly used in DDoS attacks. Through the first attack, the attackers send packets with the IP address of the target set as their source address to various destinations, this is named the reflection technique. The other mechanism is traffic amplification consisting in sending a lot of packets to the victim's computer. Both reflection and amplification techniques target the TCP/IP protocol's weaknesses using a variety of attack methods, including TCP Syn Flood, UDP Flood, ICMP Flood, and others [35].

VI. SECURITY PRECAUTIONS TO PREVENT ATTACKS

Cyber security hazards are clearly introduced by linking traditionally standalone' smart devices such as lighting, appliances and locks. A handful of parents were terrified when hackers were able to communicate with their young children through hijacked baby monitors. The following Fig. 4 is an illustration of some of the most common cyber-security threats and attacks against smart home devices. Several precautions should be followed to prevent several attacks:

A. ENSURE THAT THE ROUTER IS SET UP PROPERLY

At the network layer, household networks create a heterogeneous environment connected to the internet through a home gateway having constrained resources [36]. Moreover, when it comes to the smart home, the Wi-Fi router is the gateway. With the diversity of connected devices in the home gateway and traffic flow issues caused by security flaws on the household network, TR-069 is CPE WAN Management Protocol (CWMP) that makes it easier to monitor all online devices and ensures high-quality service. An attacker might disrupt an entire network and router. Consequently, upgrading the router is the first step to reinforcing the security of a smart home. It is the glue that holds (IoT) gadgets together and is the key to their usefulness. A secure router can be set up by following these guidelines:

1- Not naming the router with its default Name: Use a name that is not the router's model or manufacturer. The smart home network can be easily accessed if others know the brand and model of the smart home device. It is highly recommended to change it to a name that is not linked to the personal information of the home occupant, such as their identity or location.

2- Create a password that is different from the home occupant's name: set the router password to a truly unique one. It is highly recommended to make the passwords more difficult to guess by using a combination of letters, numbers, and

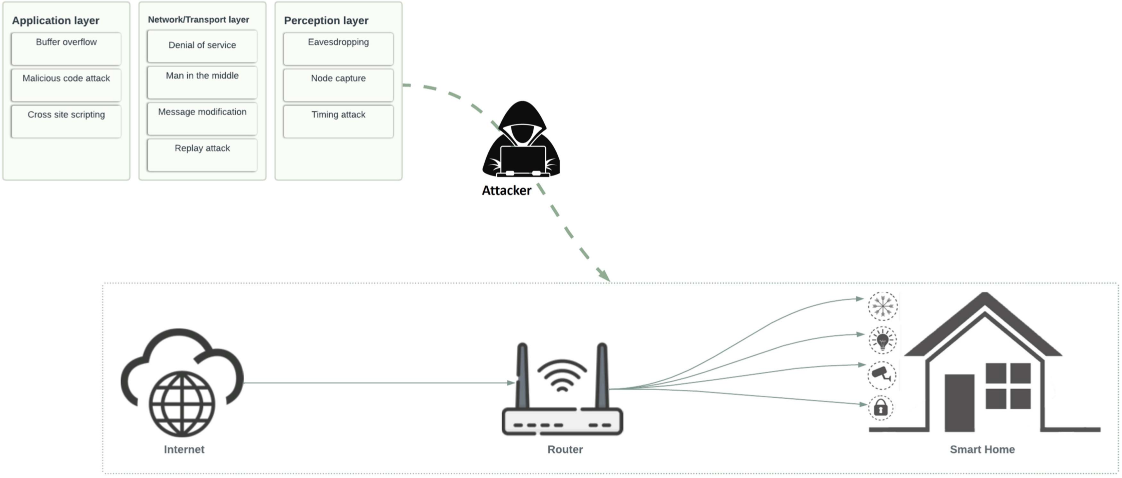

FIGURE 4. Security attacks in smart home.

other symbols. A random password generator can generate a password that is nearly impossible to crack.

3- Data Encryption: Finally, choose the most secure encryption which is WPA3 (Wi-Fi Protected Access). It tends to replace WPA2 and adds more security enhancements. By adopting the new WPA3, wireless security in the IoT environment may be protected against cracking, eavesdropping, and intrusion. Individual encryption is supported by WPA3, which makes it impossible for devices to access each other's data even when they are connected to the same network [37] Hackers focus on home routers as a prime target in the Internet of Things [38]. This means that a smart home with a secure router is far more secure.

B. ARTIFICIAL INTELLIGENT BASED HOME SECURITY WITH EDGEAI

Security cameras that feature Artificial Intelligence technology are different from other types of cameras because they are able to recognize people's faces. This innovation is useful because homeowners are allowed to see people who break into their homes and the time when an intruder commits the action. Machines or local devices run by AI algorithms allow the users to access data in real-time due to the fact that edge AI software does not require internet connections or other systems to work; there are also no problems linked to data latency. Data is processed faster and cases that work with "real-time referencing are also supported. Edge AI is important because of real-time analytics, reduced latency, higher speeds, reduced cost and bandwidth requirement, improved data security, scalability, improved reliability, and reduced power. Data is processed at the device level; this helps Edge AI to save energy costs. It is important to note that Edge AI systems are faced with a few challenges because several issues are required in their AI models. IoT devices are used in smart homes because they process and collect information from the house. The security system of a smart home can be prompted by AI to evaluate and monitor security threats. A person does not need to manually record the videos, the tasks are performed automatically by the system. The technology has devices that present different features like threat analysis and facial recognition. The system is designed to recognize faces and objects and send information about the person trying to break into the house. Advanced AI devices have facial recognition technology that recognizes pets, family members, and friends. Smoke alarms with Artificial Intelligence have smart features that are able to alert, speak, and reason on their own. Smart smoke alarms in smart homes are able to communicate with users via their smartphones' mobile applications. They are able to notify on carbon monoxide leaks, smoke, battery level, and even figure out locations with smoke and fire outbreak. Google Assistant, Siri, and Alexa are AI-enabled and can be controlled in smart homes through voice commands. It is important to note that once they make a mistake, they learn from it.

C. DEEP LEARNING-BASED HOME SECURITY

Home security and safety are crucial for occupants' well-being. A smart home automation system should integrate a security management strategy with alarms. With motion identification and detection, smart homes may be safeguarded against intruders while preventing false alarms. As walking patterns are unique to each person, IoT sensors can track human mobility and activity. The collected movement patterns offer biometric verification of humans. Accordingly, motion sensors and cameras can secure a smart house. several works suggest a motion-recognition-based home security system. This method is faster and more discrete than others. Other human detection algorithms evaluate skin tones, eye colour, and other face traits. Motion sensors detect, capture, and verify movement quietly. In [39], the authors used the CNN model to conduct an experimental examination of human motion patterns in order to assess the classification for the identification of people. The accuracy of the CNN classification model reached 99.8%.

D. MAKE THE PASSWORDS AS STRONG AS POSSIBLE

A strong password is not just important for the Wi-Fi network; it is also important for the email account and other online accounts. For example, in order to utilize IoT devices, it is mandatory to create an account and sign in. Login credentials are typically required to access the mobile apps that come pre-installed on the devices.

Every IoT device's account and application should have its own unique set of credentials. This ensures that even if one device's password is hacked; all others are safe.

When using a password manager, the user has to remember many passwords, which can be time-consuming and frustrating. If these passwords have been recorded, it is highly recommended to keep them in a safe place. It is best to utilize a password management application, which has the ability to save infinite passwords, create new ones, and sync them across many devices [40].

E. USE OF CONVOLUTIONAL NEURAL NETWORK MODEL WITHIN DEVICES

This model uses motion recognition and monitoring for home security. With CNN, surveillance camera images can be processed by detecting areas. Deep learning-based intelligent detection can help a smart home automation system categorize detected motions as occupants or intruders before triggering an alarm to the user [41]. An efficient home automation system may assist in saving energy by making sure the home makes better use of resources like water and electricity. Ambient intelligence regulates lights, entertainment systems, climate, and other home appliances.

F. CREATE AN IOT-SPECIFIC WI-FI NETWORK

A guest (or secondary) network feature is available on a large number of modern routers. The smart home occupant can protect his primary network from IoT risks by creating a secondary network for his IoT devices.

This allows guests, family members, and friends to access a network that is not connected to IoT devices. As a result, only the user and his family have access to the smart home network.

IoT devices can not access the laptop or smartphone if they are installed on a separate network, so hackers can not get into your more vital gadgets.

G. TURN OFF NEEDLESS FEATURES

Several IoT devices can operate from anywhere in the world. However, it is highly recommended to disable the remote access needless features. For instance, Smart speakers, have Bluetooth connectivity as well as Wi-Fi. Unused services could be deactivated. Also, A lot of people do not utilize their smart TVs' voice controls even if they have smart assistants like Google's Assistant, Siri's or Alexa's in their homes. Although it may seem unnerving, an active microphone can be hacked to listen to your chats. As a result, deactivating features is all about preventing as many of those various entry points as possible from being utilized [42]. Security can be enhanced in smart homes by disabling unnecessary features. Both necessary and unnecessary things can be determined by reviewing the IoT devices used in smart homes. Some devices have more features compared to others. For instance, the industrial sensor which is enabled with an IP has few features while devices oriented towards the end user have more features. Disabling a single feature helps to improve security. Some thermostats which are WIFI-enabled have a remote access feature that lets users monitor their house's temperature and make necessary adjustments. This remote access feature can be disabled not because a hacker can set the conditioner to work at full blast, but because a hacker who accesses the thermostat can use it as an avenue to launch attacks on other devices that use the same network as the thermostat.

H. REMOTE THIRD PARTY SERVICES

Remote services add functionality to the Smart Home System by analyzing and reporting the gathered data. To prevent privacy leaks, we recommend adding customizable time-resolution limit permissions to the proposed system. For more privacy, a resolution limit might prohibit access to resolutions below a 15-minute-aggregation [43]. As an optional restriction, it has little impact on usability while increasing user privacy. All API accesses and transactions should be logged to harden against compromised third-party services. If logs are automatically checked for anomalies, the user's usability is significantly impaired. Only complete and understandable documentation about the app's data processing, remote transmission, and control events should be accepted. Reviewers compare documentation to code paths and request corrections before accepting it. A user should be able to accept or reject application features before installing them. Displaying application documentation, which must be approved or rejected, is usable. In this context, GDPR (General Data Protection Regulation) has been carried out. It requires operators or vendors to take all necessary steps to safeguard users' confidentiality and privacy. In addition, they can secure or ensure the safety of a smart home using three approaches. Because the user trusts the manufacturer to pay attention to his or her data anonymization, the vendor has to apply anonymization before the collected data is stored and shared with third-party services. The information is sent clearly from the home of the user. There are some users who fail to trust the vendor to consider their data anonymization but put faith in third-party services. With regard to this approach, information is sent to a third-party service directly from the user's home. The third party acts as a middleware or proxy and is responsible for applying the anonymization; the third party has to ensure the anonymized data is forwarded to the vendor. This solution is often referred to as 'anonymization as a service. The third approach is for smart home users who fail to trust a third-party service and the vendor. According to the requirements of the smart home's user, anonymization is done locally; the process of anonymization is performed at the edge router before the information is received by the vendor.

I. UPDATING THE DEVICES IS MANDATORY

It is possible that firmware updates of the Wi-Fi router don't happen automatically. Patches for security vulnerabilities are frequently included in these releases. Check for updates manually every few months, and if any are found, it is recommended to download and install them immediately. IoT devices and applications often do not update automatically, instead informing you when new versions are available [44].

Firmware over-the-air or FOTA provides different methods aimed at updating a device's firmware without physical access because it is powering the scalability and reliability of connected devices. These updates take into account device dependencies, device parameters, trigger methods, and firmware size. Security is important when updating software, when a smart home lacks proper security, the update can easily be modified by an attacker. To improve security, smart homes should have a secure FOTA object based on a secure JavaScript Object Notation. A secure over-the-air programming framework that is based on symmetric encryption with Advanced Encryption Standards should be introduced in smart homes to keep FOTA protocols secure.

J. ACTIVATE MULTI-FACTOR AUTHENTICATION.

The term "multi-factor authentication" is familiar to everyone who has ever used online financial services. Multi-factor authentication (2FA) goes beyond a simple password to provide an additional level of protection. Every time someone tries to log into the IoT device, he must present extra evidence of their identity in order to do so.

There are some smart devices that do not have the multi-factor authentication feature by default. In this instance, other authenticators could be used to enable two-factor authentication (cloud solutions).

An extra layer of security provided by a trustworthy third-party service can give an additional piece of mind even if an IoT device has two-factor authentication with its accompanying mobile app [45].

K. SECURE M2M COMMUNICATION PROTOCOL IN IOT DEVICES

In wireless and wired technologies, the M2M technology becomes very important. M2M in smart homes provides people with an opportunity to remotely and automatically control the house. A smart house needs to be designed to accomplish multiple features and tasks like fire and gas detection, lighting, automatic door, alarm system, and temperature acquisition. Smart homes require an automation system that has been created based on the Android/Arduino UNO platform, where the brain is represented by the Arduino UNO [46]. These functions can be remotely controlled by a simple smartphone. This solution helps people to control the house, ensure comfort and safety, and use cheap and efficient sensors. A lightweight authentication mechanism that relies on XOR and hashes operations for machine-to-machine communications in an Industrial IoT environment has been proposed by experts. The mechanism which has been proposed is characterized by storage and communication overhead, and low computational cost, while achieving the device's identity confidentiality, session key agreement, mutual authentication, as well as resistance against possible attacks which include modification attacks, impersonation attacks, man-in-the-middle attacks, and replay attacks. Two procedures were used to determine the proposed mechanism which was inspired by [47]. One of the procedures is about the sensor being registered to the Authentication Server. The registration procedure needs to be performed by each sensor via a secure channel. The second authentication procedure involves mutual authentication between the router and the server. Each sensor can authenticate to a router after the registration phase. It is important to note that during the authentication procedure, sensors do not use their real identity when authenticating to a router. Hence, the sensors of the smart ID cannot be attacked by a malicious entity [47].

L. MAKE USE OF A NEXT-GENERATION FIREWALL (NGFW)

It is possible that the firewall included in the router is not up to the task. Malware protection, content filtering, SSL/SSH intercept, QoS management, and virtual private network (VPN) interception are all missing from standard firewalls (VPN).

With an NGFW, it is possible to get a firewall and all the other security features in a typical firewall, all in one integrated network platform [48]. In addition to standard firewall features, an NGFW can detect and guard against cyber-attacks. The cost of next-generation firewalls is high, but they provide a significant increase in security for smart homes. In the end, if the user can afford the gadgets, he can afford to pay a little extra to protect them. He is protecting his privacy by doing so.

Recently, several researchers recently suggested using SDN to provide users at home access to firewall functions and enhance the smart home network's administration and access control. In [49] the authors suggest an SDN, FPGA-accelerated based architecture to protect smart home networks by using K-Nearest Neighbor (KNN) based device classifications and malicious traffic detection utilizing an FPGA. In order to provide reliability, high availability, security, and safety in smart homes, NFV technologies, which considerably enhance IoT network security are adapted. A recent work [50] has inspired the proposed architecture to evaluate VNFs that can increase the security of the IoT ecosystem utilizing IoT devices like smart cameras, smart sockets, etc. The edge-analysis VNF was trained using real-time traffic from a TP-Link camera and is now capable of detecting threats with about 95% accuracy in under a second. With the use of the proper VNFs, known attacks are neutralized.

VII. CONCLUSION

In conclusion, we can assert that our personal information should be kept private exclusively within our residences. Smart homes, as opposed to conventional homes, can keep sensitive and vital information about the user while also boosting his comfort and quality of life [51]. Moreover, IoT manufacturers' powerhouses are creating smart devices without paying proper attention to security in an effort to capture the open market. Due to this conundrum and the resource limitations of IoT devices, low-power smart devices cannot be protected using typical host-based protection solutions like anti-virus, IDS, IPS, etc. In this study, we covered some of the most serious challenges related to privacy and security in a smart home and the various safety measures offered by other researchers. In addition, we did an examination of the major smart home components that must be safeguarded. We will build a robust solution to increase the degree of security in smart homes in the near future.

REFERENCES

[1] S. Madakam, "Internet of Things: Smart things," *Int. J. Future Comput. Commun.*, vol. 4, no. 4, pp. 250–253, 2015.

[2] "Smart home - statistics & facts kernel description," 2022. [Online]. Available: http://www.statista.com/topics/2430/smart-homes/#dossier Keyfigures

[3] T. S. Gunawan, I. R. H. Yaldi, M. Kartiwi, and H. Mansor, "Performance evaluation of smart home system using Internet of Things," *Int. J. Elect. Comput. Eng.*, vol. 8, no. 1, 2018, Art. no. 400.

[4] V. Jyothi, M. G. Krishna, B. Raveendranadh, and D. Rupalin, "IoT based smart home system technologies," *Int. J. Eng. Res. Develop.*, vol. 13, no. 2, pp. 31–37, 2017.

[5] S. Singh, I.-H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-blockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, 2019, Art. no. 1550147719844159.

[6] J. Kim, "Cloud Internet of Things for the smart environment of a smart city," M.S. thesis, Dept. Inf. and Decision Sci., California State Univ., San Bernardino, CA, USA, 2021.

[7] R. Heartfield et al., "A taxonomy of cyber-physical threats and impact in the smart home," *Comput. Secur.*, vol. 78, pp. 398–428, 2018.

[8] H. Kopetz, "Internet of Things," in *Real-Time Systems*. Berlin, Germany: Springer, 2011, pp. 307–323.

[9] "10 IoT security concerns to keep in mind before developing apps kernel description," 2022. [Online]. Available: https://www.peerbits.com/blog/10-iot-security-concerns-to-keep-in-mind-before-developing-apps.html

[10] A. Arora, A. Kaur, B. Bhushan, and H. Saini, "Security concerns and future trends of Internet of Things," in *Proc. 2nd Int. Conf. Intell. Comput., Instrum. Control Technol.*, 2019, vol. 1, pp. 891–896.

[11] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, 2016, Art. no. 44.

[12] Y. Lu and L. D. Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[13] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors*, vol. 18, no. 3, 2018, Art. no. 817.

[14] U. Saxena, J. Sodhi, and Y. Singh, "An analysis of DDoS attacks in a smart home networks," in *Proc. IEEE 10th Int. Conf. Cloud Comput., Data Sci. Eng.*, 2020, pp. 272–276.

[15] T. A. Abdullah, W. Ali, S. Malebary, and A. A. Ahmed, "A review of cyber security challenges attacks and solutions for Internet of Things based smart home," *Int. J. Comput. Sci. Netw. Secur*, vol. 19, no. 9, 2019, Art. no. 139.

[16] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of IoT devices: A smart home case study," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10102–10110, Oct. 2020.

[17] K. Ghirardello, C. Maple, D. Ng, and P. Kearney, "Cyber security of smart homes: Development of a reference architecture for attack surface analysis," in *Proc. Living in the Internet of Things: Cybersecur. IoT*, 2018, pp. 1–10.

[18] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet Things*, vol. 1, pp. 81–98, 2018.

[19] Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, "Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 53–59, Dec. 2018.

[20] E. Akanksha, A. Debnath, and B. Dey, "Extensive review of cloud based Internet of Things architecture and current trends," in *Proc. IEEE 6th Int. Conf. Inventive Comput. Technol.*, 2021, pp. 1–9.

[21] D. Valtchev and I. Frankov, "Service gateway architecture for a smart home," *IEEE Commun. Mag.*, vol. 40, no. 4, pp. 126–132, Apr. 2002.

[22] B. D. Davis, J. C. Mason, and M. Anwar, "Vulnerability studies and security postures of iot devices: A smart home case study," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10102–10110, Oct. 2020.

[23] T. Pattanasri, "Mandatory data breach notification and hacking the smart home: A legal response to cybersecurity," *QUT L. Rev.*, vol. 18, pp. 268–289, 2018.

[24] P. Siddhanti, P. M. Asprion, and B. Schneider, "Cybersecurity by design for smart home environments," in *Proc. 21st Int. Conf. Enterprise Inf. Syst.*, 2019, pp. 587–595.

[25] A. Karampogias, "Internet of Things and smart homes: Cyber security and personal data protection in a fragile environment," Master's thesis, Dept. of Digital Syst., Univ. of Piraeus, Piraeus, Greece, 2021.

[26] F. Hall, L. Maglaras, T. Aivaliotis, L. Xagoraris, and I. Kantzavelou, "Smart homes: Security challenges and privacy concerns," 2020, *arXiv:2010.15394*.

[27] E. Zeng, S. Mare, and F. Roesner, "End user security and privacy concerns with smart homes," in *Proc. 13th Symp. Usable Privacy Secur.*, 2017, pp. 65–80. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng

[28] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2017, pp. 103–117.

[29] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the Internet of Things," *Procedia Comput. Sci.*, vol. 175, pp. 591–596, 2020.

[30] K. Pranathi, S. Kranthi, A. Srisaila, and P. Madhavilatha, "Attacks on web application caused by cross site scripting," in *Proc. 2nd Int. Conf. Electron., Commun. Aerosp. Tech.*, 2018, pp. 1754–1759.

[31] G. E. Rodríguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (XSS) attacks and mitigation: A survey," *Comput. Netw.*, vol. 166, 2020, Art. no. 106960.

[32] K. Somasundaram and K. Selvam, "IoT–attacks and challenges," *Int. J. Eng. Tech. Res*, vol. 8, no. 9, pp. 9–12, 2018.

[33] P. Mann, N. Tyagi, S. Gautam, and A. Rana, "Classification of various types of attacks in IoT environment," in *Proc. 12th Int. Conf. Comput. Intell. Commun. Netw.*, 2020, pp. 346–350.

[34] B. Xu et al., "A security design for the detecting of buffer overflow attacks in IoT device," *IEEE Access*, vol. 6, pp. 72862–72869, 2018.

[35] E. Džaferović, A. Sokol, A. A. Almisreb, and S. M. Norzeli, "Dos and DDoS vulnerability of IoT: A review," *Sustain. Eng. Innov.*, vol. 1, no. 1, pp. 43–48, 2019.

[36] A. Camphouse and L. Ngalamou, "Securing a connected home," in *Proc. IEEE 10th Annu. Ubiquitous Comput., Electron., Mobile Commun. Conf.*, 2019, pp. 0250–0256.

[37] H. Kim and J. Song, "Analysis of IoT security in Wi-Fi 6," *J. Inst. Convergence Signal Process.*, vol. 22, no. 1, pp. 38–44, 2021.

[38] N. Vlajic and D. Zhou, "IoT as a land of opportunity for DDoS hackers," *Computer*, vol. 51, no. 7, pp. 26–34, 2018.

[39] O. Taiwo, A. E. Ezugwu, O. N. Oyelade, and M. S. Almutairi, "Enhanced intelligent smart home control and security system based on deep learning model," *Wireless Commun. Mobile Comput.*, vol. 2022, 2022, Art. no. 9307961.

[40] F. Zinggeler, "Nokey-A distributed password manager," Ph.D. dissertation, M.S. thesis, ETH Zürich, Zürich, Switzerland, 2018.

[41] R. Kishore, U. R. Vigneshwari, N. Prabagarane, K. Savarimuthu, and S. Radha, "IoT based intelligent control system for smart building," in *Proc. Int. Conf. Innov. Intell. Informat., Comput., Technol.*, 2020, pp. 1–6.

[42] A. K.Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, Jun. 2006.

[43] A. Brauchli and D. Li, "A solution based analysis of attack vectors on smart home systems," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun.*, 2015, pp. 1–6.

[44] S. McIlroy, N. Ali, and A. E. Hassan, “Fresh apps: An empirical study of frequently-updated mobile apps in the Google Play store,” *Empirical Softw. Eng.*, vol. 21, no. 3, pp. 1346–1370, 2016.

[45] V. Adat and B. B. Gupta, “Security in Internet of Things: Issues, challenges, taxonomy, and architecture,” *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2018.

[46] T. Jiang, M. Yang, and Y. Zhang, “Research and implementation of M2M smart home and security system,” *Secur. Commun. Netw.*, vol. 8, no. 16, pp. 2704–2711, 2015.

[47] A. Esfahani et al., “A lightweight authentication mechanism for M2M communications in industrial IoT environment,” *IEEE Internet Things J.*, vol. 6, no. 1, pp. 288–296, Feb. 2019.

[48] S. Thomason, “Improving network security: Next generation firewalls and advanced packet inspection devices,” *Glob. J. Comput. Sci. Technol.*, vol. 12, 2012, Art. no. E13.

[49] H. Gordon, C. Park, B. Tushir, Y. Liu, and B. Dezfouli, “An efficient SDN architecture for smart home security accelerated by FPGA,” in *Proc. IEEE Int. Symp. Local Metrop. Area Netw.*, 2021, pp. 1–3.

[50] M. Bhuyan et al., “A survey on blockchain, SDN and NFV for the smart-home security,” *Internet Things*, vol. 20, 2022, Art. no. 100588.

[51] G. Mantas, D. Lymberopoulos, and N. Komninos, “Security in smart home environment,” in *Wireless Technologies for Ambient Assisted Living and Healthcare: Systems and Applications*. Hershey, PA, USA: IGI Global, 2011, pp. 170–191.