Securing the Connected Home: Addressing Challenges, Demands, Safeguards, and Emerging Patterns in Embedded IoT Cybersecurity

Prof.Sir.Bashiru Aremu **Mohd Abdul Nayeem**

Professor & Vice Chancellor, Crown University Int'l Chartered inc.(CUICI) USA

Research Schalor,Department of Computer Science & Engineering, CUICI, USA

Abstract

To improve people's lives and offer new services, sensors and connected gadgets send data over the Internet. To monitor many parameters and improve the quality of life for its residents, smart houses employ multiple interconnected gadgets. Notably, these smart gadgets use many Internet of Things (IoT)s to install smart locks, detect smoke, automatically control lights, and monitor room temperature. However, other security and privacy issues with smart home devices include the ability for surveillance equipment to access user data and the possibility of false fire alarms. Although smart home systems make people's lives easier and maintain their safety within their houses, they are susceptible to several types of attacks. IoT cybersecurity in smart homes is the focus of this survey. The architecture, layers, and standards of IoT will be covered. We will also discuss several threats that target smart home devices, the security issues associated with smart homes, and the tiered Internet of Things framework. Next, various defence strategies against these attacks at various abstraction levels will be presented.

1. Introduction

The term "Internet of Things" (IoT) refers to "an open and comprehensive network of intelligent objects with the ability to share information, data, and resources, auto-organize, and react and act in response to external changes and situations" [1]. IoT is a cutting-edge technological advancement that is altering our way of life. A self-sufficient smart home is furnished with integrated devices, such as motion detection systems, temperature monitoring devices, light and fingerprint sensors, gas detection systems, smoke detectors, and home security cameras, that are intended to identify and react to human presence and requirements. There are numerous reasons why these gadgets are linked together, including lowering energy expenses, cutting down on bills, for the safety of those who live there [2]. To operate various sensors and equipment in these systems, users use interface devices such as computers, smartphones, or remote control [3]. IoT-enabled smart home systems are becoming increasingly popular globally to help people live more conveniently, comfortably, and smoothly [4]. (5). The most recent reports from IoT Analytics state "IoT Analytics projects that by 2021, there will be 12.3 billion active endpoints worldwide, a 9% increase in connected IoT devices. It is projected that there will be about 27 billion IoT connections by 2025 [6]. The spectrum of attack surface expands in tandem with the enormous growth in the number of connected devices, and security vulnerabilities may serve as the weakest link and serve as an entrance point for attacks. Additionally, these gadgets converse they are connected to the home internet service and can communicate directly or indirectly with one another via a variety of protocols, including Bluetooth, Wi-Fi, Zigbee, and others. In recent years, IoT network designers have faced an increasingly complicated and cutting-edge problem in securing these kinds of communications, devices, and applications. (7).

All the linked sensors and appliances in a smart home are managed by a single central monitoring endpoint, which could be a computer, tablet, smartphone, or other device. Doors, locks, air conditioners, gadgets, thermostats, screens, lights, cameras, and refrigerators are among the "things" that can be controlled. The

communication between smart home gadgets is depicted in Figure 2. Smart home appliances are often internet-connected and can be operated from a distance, for example, through a mobile application or cloud service. Because of its scalability in terms of consumption, this is very handy for the customer and can save expenses, but it can also cause issues [8]. Generally, users can utilise a desktop or mobile application to monitor and regulate these devices' security. Users are afraid that hackers may acquire credit card details used for automated retail orders, health monitoring systems, and other private and secret data. They could also operate air conditioning and lower refrigerator temperatures, damaging property.

This is how the remainder of the paper is structured. We shall talk about the issue of cyber-security in smart homes in section 2. Section 3 discusses the most current surveys and research evaluating assaults on smart home devices. Section 4 introduces the design of smart homes, while Section 5 goes into greater detail on security concerns. The next section, number 6, discusses the several layers of preventative measures for these attacks. In section 7, conclusions and viewpoints are finally highlighted. The survey's layout is displayed in Figure 1.

2. The Problem statement

Over the past few decades, the internet has expanded significantly and evolved into a need. Berners-Lee was a key figure in the creation of the World Wide Web and the internet. Berners-Lee contends that the Internet of Things (IoT) ought to be publicly accessible, free, and open to all users. By 2025, it is anticipated that 24 billion gadgets will be in the public domain and online. If these devices are not adequately protected or configured, a number of major issues could arise. Numerous connected devices gather various personal data, including name, date of birth, address, credit card information, and more, for several million dollars. This data could have an impact on the company-customer relationship in terms of customer trust and brand value [9] [10]. Ransomware is becoming more common; in the US, 11% of businesses paid a $1 million ransom in 2021. Hackers are not making it cheap; 34% of organisations used to pay less than $10,000, but that percentage has since dropped to 21%.

Sensitive information is unintentionally released due to a number of threats. For example, private health information belonging to a particular home may be made public due to a breach in a smart home system. Unauthorised access to a system controller at the administrator level is another vulnerability that renders the system as a whole insecure [11]. Furthermore, there are multiple attack surfaces and potential weaknesses on these networked devices. By infecting the machine with malware or gaining direct access to the control panel, numerous assaults can be executed remotely.

The most significant cyber-security issues with IoT devices utilised in smart, networked houses are the major topic of this article. We're going to present a taxonomy of IoT device vulnerabilities, threats, and attacks. Additionally, we will highlight a number of security solutions that are suggested and countermeasures that may be applied to keep IoT networks, applications, and devices cybersafe and defend them against cyberattacks. The work's innovation keys are as follows:

1) extending research on smart home system intrusions and architecture.

2) We handle several types of attacks that we categorise into three distinct system tiers.

3) We discuss how to exploit the sensor and other smart home devices.

The primary research topics we are addressing because this effort focuses on embedded IoT security challenges especially are as follows:

- (Q1): What makes a smart home architecturally sound?
- (Q2): What are the primary security issues and vulnerabilities with smart home systems?
- (Q3): Which sensors are under attack within the perception layer?
- (Q4): Which assaults target networks and communication?
- (Q5): In a smart home, how are sensors, appliances, or actuators protected from device attacks?
- (Q6): How do contemporary smart homes (endpoints and gateways) defend themselves against software application attacks?
- (Q7): In terms of protecting Smart Home systems, what are the open viewpoints and future research directions?

3. Associated Works

Several research projects aim to take advantage of security holes in IoT devices in order to understand the illness, provide a workable solution for the Internet of Things and Smart Home environments that will quickly identify symptoms (IDS), provide treatment, and ultimately safeguard the patient. A cyberattack attempts to alter, remove, intercept, modify, or pilfer data. Additionally, it might damage or abuse a network. Several approaches are intended to be used, and tools are being developed to guard against malicious threats that could take control of smart home devices and steal data from them. Smart home appliances are vulnerable to a variety of assaults, including Man-in-the-Middle, Data Breach,

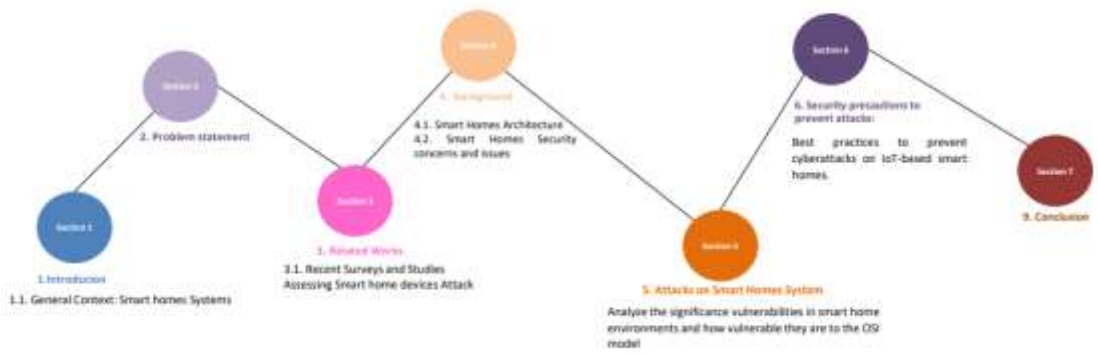

Figure 1 Organization of the review paper

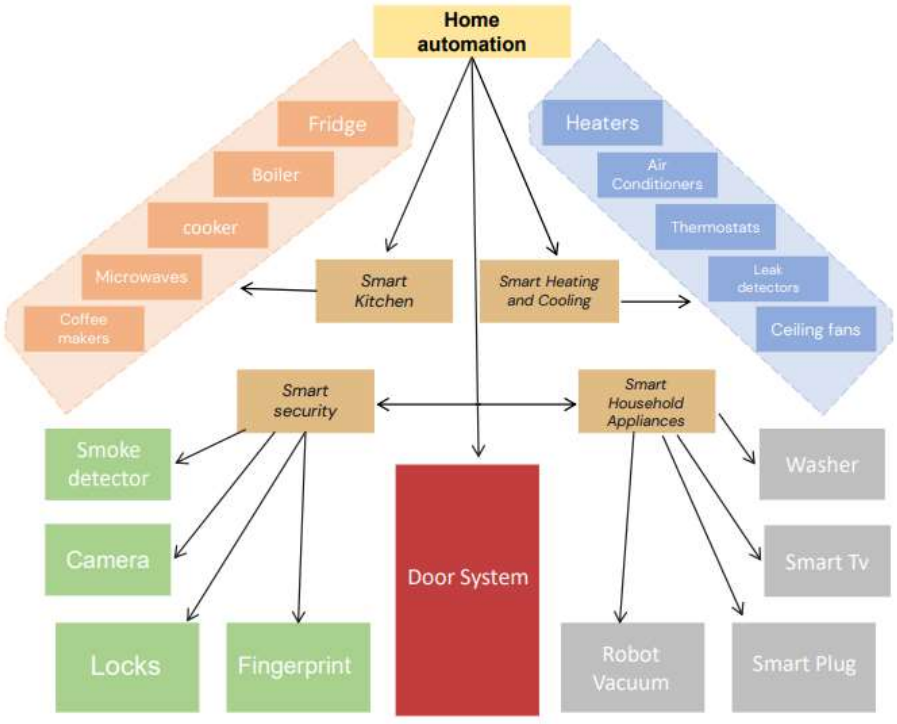

Figure 2 Smart home devices communications

Distributed Denial of Service (DDoS), spoofing, identity theft, and device hijacking. The three categories of security attributes that these assaults fall under are availability, integrity, and secrecy. We shall review a number of current papers concerning smart home security issues in this part.

The authors of [12] described every layer of their suggested four-layered cybersecurity-oriented architecture, which is specifically designed for Internet of Things devices. The layers include sensing, networking, middleware, and application. The authors also specify the kind of assault that targets each tier. Furthermore, they

divide various attacks into eight groups: main attacks, protocol-based, layer-based, device, location, access level, information damage level, host promise, and strategy. The authors discussed many research issues and future developments in addition to summarising the various IoT designs from a security standpoint.

The authors of [12] described every layer of their four-layered cybersecurity-oriented architecture sensing, networking, middleware, and application for Internet of Things devices. The authors also specify the kind of assault that targets each tier. Furthermore, they investigated the primary countermeasures for IoT security from a layer-level viewpoint. The authors discussed many research difficulties and future prospects in addition to summarising the important applications in industries.

In order to detect security threats and possible hazards in an Internet of Things (IoT)-based smart home environment, Ali et al. [13] introduced OCTAVE Allegro, a novel approach that primarily focuses on information assets. They also construct risk scores for these objectives and discuss the implications and possible effects of these hazards. From an IoT-based smart home standpoint, their goal was to develop a framework for identifying and evaluating security threats.

Saxena et al. outlined the various forms of assaults on smart home networks in [14] and divided them into two categories: passive attacks and active attacks. The authors also improved the categories of Distributed Denial of Service Attacks and provided a list of several technologies that are utilised in Smart Home Networks, both internally and outside. In this work, the experimental setup concentrated on identifying and mitigating DDoS attacks by extracting network traffic as input data using Wireshark. These include the length of the attack, the response time, the downtime of the server, the port and protocol utilised, the DNS type, and the packet length. Following feature extraction, they locate the choke node and create a graph based on the attack threshold. Lastly, they use the algorithm of the shortest way to counteract DDoS attacks.

According to Abdullah et al. [15], there are only six major vulnerabilities that lead to widespread vulnerabilities: antiquated protocols, bad encryption, insufficient storage and CPU, unsecured applications, inadequate authentication, and firmware failure. Threats included denial of service (DoS), eavesdropping, impersonation, compromise, and malicious software in smart home networks, to name only four or five major danger categories. The best user practises and suggested security measures, such as software updates, frequent password changes, and network monitoring, were covered in this article for smart home setups.

The authors outline the main weaknesses in smart home technology in [16]. They categorise the attacks into four primary groups: software, encryption, networks, and physical attacks. Moreover, find out whether any vulnerabilities of any kind have been found in the particular IoT devices. Although the initial vulnerability research compares two distinct devices, more evidence is needed. They thus investigate four items in the same utility category smart lighting. Most vulnerability evaluations concentrate on well-known suppliers and products. Their tests show that devices from well-known vendors have stronger security postures than those from less well-known vendors.

The smart home system architecture is presented in the subsequent sections of this article. Next, at several levels of abstraction application, transport, network, and perception we draw attention to its various security flaws and issues. We next talked about future directions and uncharted territory in the field of smart home system security research.

4. Background: Security concerns and the architecture of smart houses

A. Smart house design

Smart homes have developed into places where gadgets with an Internet connection may operate and keep an eye on domestic appliances and systems. These devices, which are equipped with sensors, actuators, software, and data processing capabilities, are collectively referred to as the Internet of Things (IoT). Originally used as a kind of remote on/off switch, smart home appliances have developed into gadgets that can control our houses according to pre-established patterns, scenarios, or user preferences. There are numerous layers in the architecture of the Internet of Things Smart Home, including perception, transport, network, and applications. [17, 18]. These layers attempt to give a service, access, connection, and management of items via the Internet at any time and from any location. Rather than being different and unrelated, they complement one another [17]. The physical component of the smart home environment that houses the hardware devices is the focus of the perception layer. One physical resource that can monitor environmental factors like motion, light, doors, and temperature is a sensor. It gathers data and sends it to devices via a network [18]. The transport layer should handle the transmission procedure [19]. each other [17] and seek to offer a service, access, and management of

things through the Internet from anywhere at any time. The physical component of the smart home environment, which includes hardware devices, sensors, and actuators, is the focus of the perception layer. One physical resource that may gather data from real-world settings, such as motion, light, doors, and temperatures, is a sensor. This data is then collected and sent to devices via a network [18]. The transport layer should handle the transmission procedure [19].

The application layer will allow devices to be remotely monitored or to dashboard data received from the devices. The network layer is in charge of sending gathered data to the application or processing unit [20].

Figure 3 shows an example of the architecture of a multi-layered smart home system.

The information is sent across the network in the following ways: via LPWAN (low power wide area network),

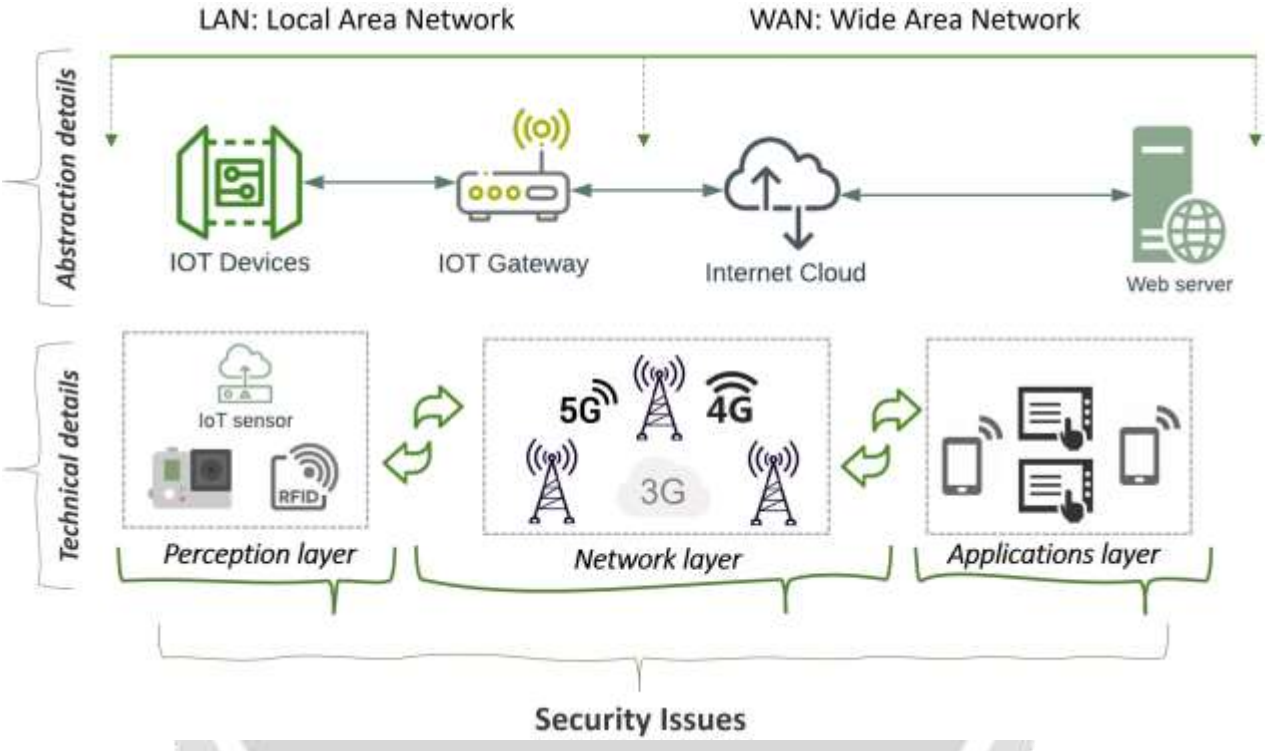

Figure 3. Architecture of IoT system

and devices wirelessly send data to a cloud platform. The two protocols that Cloud IoT Core supports for effective data transfer are MQTT and HTTP. Devices connect to Cloud IoT Core over either the HTTP or MQTT bridge.

The information obtained from the wireless sensor network will also be uploaded via gateways to cloud storage. User access to the data is granted once it has been acquired and is kept in cloud storage. The components of the cloud solution include a front-end application, storage devices, and a back-end application. Specific cloud engines (like Google App Engine) or on-site workstations are used for the back-end processing and analysis of the data. The user can manage services and devices and view the environment through a web or mobile application once the application layer is established [18]. Connecting the user to smart devices is done through the UI. Several aspects of these devices, including voice monitoring, could be monitored by the commands. The voice user interface (VUI) has recently gained the most traction because of how simple it is to use [19]. Many smart voice control devices, like Apple Siri, Google Home, Alexa, and Amazon Echo, use machine learning technology called NLP (natural language processing), which converts spoken words into written form and responds to user requests.

Moreover, a gateway device bridges and secures the communication gap between end devices, sensors, systems, and the cloud [17]. The gateway is effectively utilised to monitor and authenticate communication between IoT devices in the system, as well as to remotely control home appliances. Either the gateway or devices at the perception layer may be controlled by the mobile device [21]. As a result, information is sent from the sender to the recipient via the gateway. The IoT possesses sufficient processing capacity to handle data processing at the edge of the network before sending it to the cloud [15]. Additionally, by connecting end devices to the external

network and enabling all communication to be filtered before commands reach the end devices, the gateway strengthens the security of the smart home network [18].

B. Security problems and concerns with smart homes

People are being compelled to adjust to a comfortable lifestyle enabled by smart home devices due to developments in technology and innovation. Smart home appliances are prone to cybersecurity hazards even if they are easy to use and provide several benefits for security and safety concerns [22]. 23]

Indeed, a number of incidents show that intelligent home automation has been repeatedly hacked due to user error and several device vulnerabilities [24]. This increases the likelihood that people who heavily rely on smart home automation may worry about cybersecurity. People must continue to be worried about their security and safety procedures, particularly in light of the growing importance of smart home automation [25]. It is necessary to perform improved network-based process evaluations, threat area analyses, and cybersecurity framework assessments. The inadequate user manual makes it easy for hackers to bypass the security system's built-in security safeguards, which can then take down the entire network of the smart home automation system [26]. It's important to keep in mind that there's a chance that flaws could compromise the security of smart devices, which could lead to physical attacks directed towards them [23]. By placing subpar sensors and messing with digital connections, smart houses are also vulnerable to physical attacks. Furthermore, even though the activation of the external processes may not seem hazardous, the actual risk arises when the devices are turned on. Because there is insufficient proof and control over the security of the hardware and software systems of the devices, these physical attack problems have an impact on data integrity [26].

5. Cyberattacks on Systems in Smart Homes

Numerous facets of a user's life are impacted by the rise of smart homes. They will be monitored by a range of sensors, such as microphones, cameras, motion detectors, and activity logs. Although voice-activated lighting and remote-controlled door locks are among the convenience benefits that these smart homes offer, security experts have highlighted the risks to privacy and security that come with having internet-connected equipment in a home. Among the concerns brought up are insecure communication that exposes personal information about the house and its occupants and gadget flaws that could be used by an attacker to remotely monitor or otherwise meddle in the lives of the people. In [27].

Although the goal of all these systems is to improve people's quality of life, privacy issues are brought up by data leaks. Four tiers of interconnected automation systems need to be taken into account while building a smart home:

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

Table 1 displays the assaults on smart home systems as well as the IoT devices in each tier.

I. Transport layer:

Data is sent over TCP; MQTT is intended for IoT and M2M message transport. MQTT ensures that the entire connection is encrypted by using Transport Layer Security in conjunction with IP/TCP. When it comes to streaming or event-based data, MQTT is crucial. Because MQTT may be utilised in limited applications and send payloads, it is widely employed in Internet of Things applications. Information security is ensured by UDP security features in another protocol called CoAP. CoAP employs Datagram TLS over UDP, much as HTTP uses TLS over TCP. The transport layer is vulnerable to the following attacks:

1) Replay attack: in this type of attack, a third party listens in on conversations between two reliable people and then broadcasts the information as if it came from them. An authentic service request sent from a device linked to the smart home network can be replicated and stored by the attacker. To use the service that a home user is permitted to use, play it again later.

2) Modification of messages: When external parties try to eavesdrop on authorised parties' discussions, alter information values, or change software to function maliciously, messages may be changed.

3) Denial of Service (DOS) Attacks are employed when a hacker wants to limit the availability of network services or prevent authorised users from accessing a network. To exhaust the resources of the smart home network system, the attacker can broadcast an unending stream of messages. Consequently, authorised users are unable to utilise the home network's services. Within the smart home, the intrusion can also limit internal traffic transferred through wired or wireless networks by bombarding servers and other Internet-connected devices with messages.

II. Perception layer:

It's called the sensor layer a lot. It functions similarly to the nose, hearing, and eyes of a person. It is in charge of recognising things and deriving data from them. RFID, 2-D barcode, and sensors are a few examples of information-gathering sensor kinds. The needs of the applications are taken into consideration when choosing the sensors. One type of sensor that can monitor environmental or physical changes in homes is the MEMS sensor. Furthermore, gyroscopes are used to measure rotational motion. As a result, it is capable of detecting when a window or door is opened and closed. The position sensor can identify whether people or other items are present in a given area by tracking their movements. For home security, the owner may track the doors, windows, and appliances from anywhere in the house thanks to these sensors. These sensors may gather data on position, surrounding conditions, air quality, motion, vibration, etc. Nonetheless, they are the main target of attackers trying to jam or spoof these sensors. As a result, the sensors are the target of most threats at this level. Typical security issues with the perception layer are:

1) Eavesdropping: this kind of illicit real-time assault involves the interception of private communications such as text messages, phone conversations, faxes, and video conferences by the attacker. It attempts to steal information sent via a network. Subsequently, it exploits insecure communication to obtain data that is both sent and received. Additionally, earlier research such as that pertaining to the Dolphin assault in [28] has demonstrated that attackers are capable of using inaudible speech attacks to control mobile devices and hiding their voice commands by modulating them on ultrasonic carriers. The authors of [28] tested their attack on a number of well-known speech recognition systems, including Alexa, Cortana, Samsung S Voice, Huawei HiVoice, Google Now, and Siri.

2) Node Capture: one of the most important perception layer attacks that may be applied to wireless sensor networks. It gives an attacker the ability to easily take over the entire network and can expose any sensitive security data, such as encryption keys, shared secrets, and sender-receiver interactions.

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 sensorspecific service to application/client	Take control, To identify speakers, Cross-site scripting, Malicious canr overflow

3) Playback Attack: Playback attacks, sometimes referred to as interceptor attacks. A hacker intercepts communications between a sender and a recipient in order to obtain real information from the sender [29]. An intruder uses identification and authenticity proof to provide the victim with the same verified information that they have already been given. In order for the recipient to understand the message as a legitimate request and fulfil the intruder's intention, it is encoded.

4) Timing Attacks: these are typically employed against devices with low computing power. By timing how long a system takes to react to different input, requests, or cryptographic techniques, an attacker can find holes in the system and steal confidential information.

III. Application Layer

In a heterogeneous Internet of Things context, application layer protocols are essential. They specify how Internet of Things devices and the network communicate. In a smart home setting, these gadgets might be monitored and managed by a number of applications. Access to essential personal and private data as well as the security of the entire Internet of Things could be jeopardised by a system vulnerability at the application level. Typical issues and concerns with application layer security include:

1) Cross-Site Scripting, also referred to as a Web attack, is an injection attack type. While it is not difficult to identify and detect these attacks, it might be difficult to distinguish between them and to protect against them. Usually, it targets the user-side programmes instead than the server-side ones. In [30]. It occurs when specific web applications are used to distribute or execute malicious web code, usually in script form, from the victim's computer's browser. Then, a hacker might obtain private data or take the user's cookies and utilise them for their own purposes. Additionally, give the attackers the chance to obtain private data or even take over particular machines [31].

2) Malicious Code Attack: a term used to describe any software code that aims to damage the system. An adversary may employ an end-user assault to gain entry into a system and introduce malicious malware of any kind to pilfer user data [32]. It's the kind of attack that antivirus software might not be able to stop or manage.

3) Buffer overflow: A multitude of software and hardware flaws, including buffer overflow attacks, can now affect Internet of Things devices. In a buffer overflow attack, which happens when the storage space is exceeded, a buffer acts as a temporary storage area for data [33]. The authors of [34] describe hardware architecture with architectural advancements for buffer overflow attack detection.

IV. Networking layer

To connect devices, networks, and servers, smart home gadgets make use of network layer protocols including Bluetooth, IrDA, WiFi, ZigBee, RFID, NUWB, NFC, Wireless Hart, and other communication technologies. The network layer of wireless networks is most likely to be attacked. The primary dangers associated with network communication are related to inadequate authentication and confidentiality settings. Furthermore, malicious actors conduct network eavesdropping attacks also referred to as network sniffing or network snooping attacks using vulnerable networks. A few instances of attacks are as follows:

1) Denial-of-service (DoS) Attack: A DoS attack aims to prevent legitimate users from accessing devices or other network resources. Usually, this is achieved by flooding the targeted devices or network resources with requests, which makes it difficult or impossible for some or all of the real users to utilise the equipment.

2) Man-in-the-middle (MiTM) attack: In a MiTM attack, the attacker surreptitiously listens in on the conversation between the sender and the recipient, leading both parties to believe that they are having a direct conversation. When an attacker has control over communication, they might modify communications to fit their needs. It is a major danger to internet security since it gives the attacker the ability to get information and change it instantly. Recently, a man-in-the-middle vulnerability in a Samsung smart refrigerator was discovered by a group of hackers. Hackers were able to gain access to the network and the login credentials of Gmail users by figuring out that the device does not verify SSL certificates. They were also able to monitor activity for the username and password required to link the refrigerator to Gmail.

c) Distributed denial-of-service, or DDoS, attacks are one of the biggest threats to the Internet. DDoS attacks often employ one of two methods. In the first assault, known as the reflection technique, attackers transmit packets to many destinations using the target's IP address as their originating address. The other method is called traffic augmentation, and it involves flooding the victim's PC with packets. Reflection and amplification approaches both use a range of attack techniques, such as TCP Syn Flood, UDP Flood, ICMP Flood, and others, to exploit the vulnerabilities in the TCP/IP protocol [35].

6. Security measures to avert intrusions:

By connecting traditionally solitary smart devices like locks, appliances, and lighting, cyber security risks are exposed. When hackers used baby monitors they had taken over to communicate with their young children, a few parents became very afraid. Some of the most frequent cyber-security risks and attacks against smart home devices are shown in figure 4 below. To stop multiple attacks, the following precautions should be taken:

A. Verify that the router is configured correctly:

Household networks, connected to the internet via a home gateway with limited resources, establish a diverse environment at the network layer [36]. Furthermore, the Wi-Fi router serves as the gateway in a smart home. Due to the variety of devices connected to the home gateway and the problems with traffic flow brought on by security holes in the home network, TR-069 is a CPE WAN Management Protocol (CWMP) that facilitates the monitoring of all online devices and guarantees reliable service. A router and network as a whole could be taken down by an attacker. Thus, strengthening the security of a smart home starts with updating the router. It serves as the connector between (IoT) devices and is essential to their practicality. These instructions can be used to set up a secure router:

1. Using a name other than the model or manufacturer of the router: Don't name the router with its default name. If other people are aware of the smart home device's brand and model, they can simply gain access to the smart home network. It is strongly advised that you replace it to a name that is unrelated to the resident of the house's location or identity.

2. Make sure the router password is genuinely unique by creating a password that differs from the name of the home occupant. It is strongly advised to use a combination of letters, numbers, and other symbols to make the passwords harder to guess. It is feasible to create a password with a random password generator that is almost hard to figure out.

3. Data Encryption: Lastly, select WPA3 (Wi-Fi Protected Access), which provides the most secure encryption. It tends to supersede WPA2 and offers further security improvements. The IoT environment's wireless security may be shielded against hacking, eavesdropping, and intrusion by implementing the new WPA3. WPA3 supports individual encryption, which prevents devices from accessing each other's data even when they are linked to the same network [37]. Home routers are a popular target for hackers in the Internet of Things [38]. Thus, a secure router makes a smart home much more secure.

B. EdgeAI-based artificial intelligence-based home security:

Security cameras with AI technology distinguish themselves from other kinds of cameras by having the capacity to identify faces. The benefit of this innovation is that it allows homeowners to view intruders and the exact moment they commit a break-in. Users can access data in real-time on computers or local devices powered by AI algorithms because edge AI software doesn't depend on other systems or internet connections to function, and there are no issues with data latency. Faster data processing is achieved, and "real-time referencing" scenarios are supported as well. Real-time analytics, lower latency, faster speeds, less money and bandwidth needed, better data protection, scalability, increased dependability, and lower power consumption are some of the reasons why edge AI is significant. Edge AI saves energy because data is processed at the device level. It is noteworthy that Edge AI systems have certain difficulties since their AI models need to address several problems. Because they process and gather data from the house, IoT devices are employed in smart homes. Artificial intelligence (AI) can be used to alert and guide a smart home's security system to security threats. A human

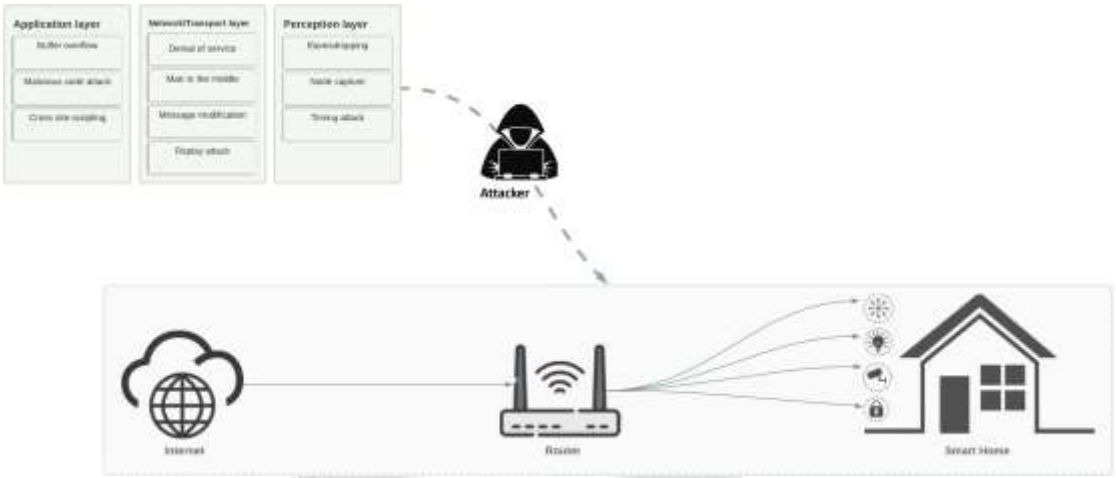

FIGURE 4. Security attacks in smart home

does not need to manually record the movies because the system takes care of all the work. Devices with various features, such as threat analysis and facial recognition, are part of the technology. The goal of the system's architecture is to identify faces and items and transmit data about the intruder. With the use of facial recognition technology, advanced AI devices can identify friends, family, and pets. Artificial intelligence-enabled smoke alarms come with intelligent capabilities that can notify, converse, and think for themselves. Users can interact with smart smoke alarms in smart homes using the mobile applications on their cellphones. They can alert users to smoke, carbon monoxide leakage, battery levels, and even the locations of fire and smoke outbreaks. Voice commands can be used to control AI-enabled devices such as Google Assistant, Siri, and Alexa in smart homes. It's crucial to remember that they learn from their mistakes.

C. Deep Learning-Based Home Security:

The safety and security of a home are essential to the wellbeing of its occupants. Alarms and a security management plan should be integrated by a smart home automation system. By using motion identification and detection, smart homes may be protected from intruders and false alarms can be avoided. Individual walking patterns allow IoT sensors to track human movement and activity. The gathered movement patterns provide biometric authentication for people. Consequently, a smart home can be secured using cameras and motion sensors. A home security system based on motion recognition is suggested in a number of works. Compared to previous methods, this one is more discrete and speedier. Additional algorithms for human detection assess facial features including skin tone and eye color. Moved Silent movement is detected, recorded, and verified by sensors. In [39], the authors experimentally examined human motion patterns using the CNN model to evaluate the classification for person identification. The CNN classification model achieved 99.8% accuracy.

D. Make the passwords as strong as possible:

A strong password is crucial for email accounts and other internet accounts in addition to Wi-Fi networks. For instance, setting up and signing in requires an account in order to use IoT devices. Usually, in order to use the pre-installed mobile apps on the devices, login credentials are needed.

Each account and application on an IoT device should have a distinct set of credentials. This guarantees that all devices are safe even in the event that a password compromise occurs on one.

It might be annoying and time-consuming for the user to have to remember numerous passwords while using a password manager. It's advised to store these passwords in a secure location if they have been recorded. The ideal option is to use a password management program, which can generate fresh passwords, store an unlimited number of passwords, and sync them across numerous devices [40].

E. Convolutional neural network model use in gadgets:

For home security, this model makes use of motion detection and monitoring. CNN can interpret photos from surveillance cameras by identifying regions. Intelligent detection based on deep learning can assist a smart home automation system in classifying motions that are detected before alerting the user to an intruder or occupant

[41]. By ensuring that the house utilizes resources like water and electricity more effectively, an effective home automation system may help reduce energy use. The climate, lights, entertainment systems, and other household appliances are all controlled by ambient intelligence.

F. Establish a Wi-Fi Network Dedicated to IoT:

Many contemporary routers include a guest (or secondary) network feature. By setting up a secondary network for his IoT devices, the owner of a smart home may safeguard his primary network against Internet of Things threats.

This makes it possible for visitors, relatives, and friends to access a network unconnected to Internet of Things devices. Consequently, the smart home network is only accessible to the user and his family.

If your laptop or smartphone is put on a different network than your IoT devices, then hackers cannot access your more important equipment.

G. Disable unnecessary features:

Numerous Internet of Things devices are global in their operation. It is, however, strongly advised to turn off the unnecessary remote access functions. For example, smart speakers are equipped with both Bluetooth and Wi-Fi connectivity. Services that are not used could be disabled. Additionally, even though many individuals have smart assistants like Google Assistant, Siri, or Alexa in their homes, many do not use the voice commands on their smart TVs. An active micro-phone can be hacked to listen in on your talks, which may seem unsettling. Deactivating features is therefore all about keeping as many of those different access points from being used as you can [42]. Disabling unused functions in smart homes can improve security. Examining the Internet of Things (IoT) devices utilized in smart homes might reveal both essential and superfluous items. In comparison to other gadgets, some have greater features. For example, a gadget geared toward the end user has many functions, whereas an industrial sensor empowered with an IP has very few. Improving security can be achieved by disabling a single feature. A remote access option on certain WiFi-enabled thermostats allows customers to check the temperature in their home and make any required adjustments. The reason this remote access feature can be disabled is not so much that a hacker can turn the air conditioner on full blast, but rather that a hacker who gains access to the thermostat can use it to launch assaults on other devices sharing the same network.

H. Remote Services from Third Parties:

By evaluating and reporting the collected data, remote services enhance the functionality of the smart home system. We advise incorporating customizable time-resolution limit permissions into the proposed system to stop privacy breaches. A resolution limit could forbid access to resolutions smaller than a 15-minute aggregate in order to provide greater privacy [43]. It improves user privacy and has minimal effect on usability as an optional limitation. Logging all API accesses and transactions is necessary to strengthen defenses against hacked third-party services. Logs that are automatically examined for irregularities greatly reduce the usefulness of the user interface. Acceptable documentation should only cover the entirety and ease of understanding of the app's data processing, remote transmission, and control events. Before accepting documentation, reviewers compare it to code paths and make correction requests. Before installing a program, the user should have the option to accept or reject its features. It is useful to display the application documentation, which needs to be accepted or denied. The General Data Protection Regulation (GDPR) has been implemented in this regard. Operators and providers must take all necessary precautions to protect users' privacy and confidentiality. They can also use three methods to secure or guarantee the safety of a smart home. The vendor must provide anonymization before the gathered data is retained and shared with third-party services since the user trusts the manufacturer to protect their privacy. The user's residence is where the information is plainly sent from. Some users rely on third-party services instead of trusting the vendor to take their data anonymization into consideration. In this method, data is transmitted straight from the user's house to a third-party provider. Applying the anonymization and making sure the vendor receives the anonymized data are the responsibilities of the third party, which serves as a middleman or proxy. Anonymization as a service is a common term used to describe this approach. For consumers of smart homes who don't trust the vendor or a third-party service, there is a third option. Anonymization is done locally based on the user's requirements for the smart home; it is done at the edge router prior to the vendor receiving the information.

I. The gadgets must be updated:

It's conceivable that the WiFi router's firmware isn't updated automatically. These releases usually contain security vulnerability patches. Every few months, manually check for updates. If any are identified, download and install them right away. IoT apps and devices frequently notify you when new versions are available rather than updating automatically [44].

Because it powers the scalability of devices, firmware over-the-air, or FOTA, offers many techniques for updating a device's software without requiring physical access and the dependability of linked devices. These modifications consider firmware size, trigger techniques, device parameters, and device dependencies. Software updates require security because an insecure smart home makes it easy for an attacker to alter the update. A safe JavaScript Object Notation should serve as the foundation for a secure FOTA object in smart homes to increase security. To maintain the security of FOTA protocols in smart homes, a secure over-the-air programming framework built on symmetric encryption using Advanced Encryption Standards should be implemented.

J. Activate Multi-Factor Authentication:

Anyone who has ever used online financial services is familiar with the term "multi-factor authentication." Apart from a password, multi-factor authentication (2FA) adds another layer of security. An additional form of identity verification must be presented each time an individual attempts to log into the Internet of Things device.

Certain smart devices are not equipped by default with multi-factor authentication. In this case, two-factor authentication (cloud solutions) could be enabled using different authenticators.

Even if an IoT device has two-factor authentication with its companion mobile app, an additional layer of security offered by a reliable third-party service can offer additional peace of mind [45].

K. Safe M2M protocol for Internet of Things devices:

When it comes to both wired and wireless technologies, M2M technology becomes crucial. M2M in smart homes gives users the ability to control the house automatically and remotely. Multiple features and functions, such as automatic doors, temperature acquisition, lighting, gas and fire detection, and alarm systems, must be included in the design of a smart home. An automation system designed for smart homes must be built on the Android/Arduino UNO platform, in which the Arduino UNO serves as the brain [46]. A basic smartphone can be used to operate these features remotely. This solution makes it easier for consumers to utilize affordable and effective sensors, regulate the house, and guarantee comfort and safety. Experts have devised a lightweight authentication system for machine-to-machine interactions in an Industrial IoT setting that uses XOR and hashing operations. The suggested mechanism achieves the de- vice's identity confidentiality, session key agreement, mutual authentication, and resistance against potential attacks, such as modification attacks, with minimal computational cost and minimal overhead in storage and communication attacks using impersonation, replay, and man-in-the-middle techniques. The suggested mechanism was ascertained by two processes that drew inspiration from [47]. A process involves registering the sensor with the authentication server. Every sensor must complete the registration process over a secure channel. The router and the server must mutually authenticate in order to complete the second authentication process. Once registration is complete, each sensor can authenticate to a router. It is significant to remember that when sensors authenticate to a router, they do not use their true identities during the process. As a result, an adversary cannot attack the smart ID's sensors [47].

L. Employ Next-Generation Firewall Technology (NGFW):

It's likely that the router's built-in firewall is inadequate for the job. Standard firewalls lack QoS management, content filtering, SSL/SSH intercept, malware protection, and virtual private network (VPN) interception.

An NGFW allows for the integration of a firewall and all other security capabilities included in a standard firewall onto a single, integrated network platform [48]. Apart from the functionality found in a normal firewall, an NGFW has the ability to identify and prevent cyberattacks. Although next-generation firewalls are expensive, they give smart homes a much higher level of protection. If the consumer can ultimately afford the devices, he can also afford to spend a little bit more to keep them safe. By doing this, he is preserving his privacy.

Several academics have proposed utilizing SDN to improve the administration and access control of smart home networks and give users at home access to firewall services. The authors of [49] propose an SDN, FPGA-accelerated architecture that uses malicious traffic detection with the help of an FPGA and K-Nearest Neighbor (KNN) based device classifications to safeguard smart home networks. NFV technologies, which may improve IoT network security, are adopted to give smart homes with dependability, high availability, security, and safety. The suggested architecture to assess VNFs that can improve the security of the IoT ecosystem by employing IoT devices like smart sockets, cameras, and other smart devices was inspired by a recent work [50]. After being trained on real-time traffic from a TP-Link camera, the edge-analysis VNF can identify threats in less than a second with an accuracy of roughly 95%. The right VNFs are used to neutralize recognized attacks.

7. Conclusion:

Finally, we may state that private information about us should only be disclosed inside our homes. Smart homes are different from traditional houses, can improve a user's comfort and quality of life while simultaneously preserving sensitive and important information about them [51]. In addition, giants in the IoT industry are producing smart gadgets with inadequate security consideration in an attempt to take market share. Low-power smart devices cannot be protected by standard host-based protection solutions such as anti-virus, IDS, IPS, and so on because of this paradox and the resource constraints of IoT devices. We discussed some of the most important issues surrounding security and privacy in smart homes in this study, as well as the different safety precautions that other researchers have suggested. We also looked at the main components of smart homes that need to be secured. In the near future, we will develop a strong solution to raise the level of security in smart homes.

REFERENCES:

[1] S. Madakam, "Internet of things: smart things," *International journal of future computer and communication*, vol. 4, no. 4, p. 250, 2015.

[2] "Smart home - Statistics Facts kernel de- scription," ://www.statista.com/topics/2430/smart- homes/dossierKeyfigures.

[3] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Hybrid Serial-Parallel Linkage Based six degrees of freedom Advanced robotic manipulator. *Computer Integrated Manufacturing Systems*, *29*(2), 70–82. Retrieved from http://cims-journal.com/index.php/CN/article/view/786

[4] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Novel Energy Storage Material and Topologies of Computerized Controller. *Computer Integrated Manufacturing Systems*, *29*(2), 83–95. Retrieved from http://cims-journal.com/index.php/CN/article/view/787

[5] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Advanced robotic manipulator renewable energy and smart applications. *Computer Integrated Manufacturing Systems*, *29*(2), 19–31. Retrieved from http://cims-journal.com/index.php/CN/article/view/782

[6] Umakant Dinkar Butkar, Manisha J Waghmare. (2023). Crime Risk Forecasting using Cyber Security and Artificial Intelligent. *Computer Integrated Manufacturing Systems*, *29*(2), 43–57. Retrieved from http://cims-journal.com/index.php/CN/article/view/784

[7] Umakant Dinkar Butkar, Dr. Pradip Suresh Mane, Dr Kumar P K, Dr. Arun Saxena, Dr. Mangesh Salunke. (2023). Modelling and Simulation of symmetric planar manipulator Using Hybrid Integrated Manufacturing. *Computer Integrated Manufacturing Systems*, *29*(1), 464–476. Retrieved from http://cims-journal.com/index.php/CN/article/view/771

[8] H. Kopetz, "Internet of things," in *Real-time systems*. Springer, 2011, pp. 307–323.

[9] "10 IoT security concerns to keep in mind before developing apps kernel description," ://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 *2019 2nd international conference on intelligent computing, instrumenta- tion and control technologies (ICICICT)*, vol. 1. IEEE, 2019, pp. 891–896.

[11] H. Lin and N. W. Bergmann, "Iot privacy and security chal- lenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[12] Y. Lu and L. Da Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2103–2115, 2018.

[13] B. Ali and A. I. Awad, "Cyber and physical security vulnera- bility assessment for iot-based smart homes," *sensors*, vol. 18, no. 3, p. 817, 2018.

[14] U. Saxena, J. Sodhi, and Y. Singh, "An analysis of ddos attacks in a smart home networks," in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, 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, p. 139, 2019.

[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 of Things Journal*, vol. 7, no. 10, pp. 10 102–10 110, 2020.

[17] K. Ghirardello, C. Maple, D. Ng, and P. Kearney, "Cyber secu- rity of smart homes: Development of a reference architecture for attack surface analysis," in *Living in the Internet of Things: Cybersecurity of the IoT-2018*. IET, 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 of 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 Communications*, vol. 25, no. 6, pp. 53–59, 2018.

[20] E. Akanksha, A. Debnath, and B. Dey, "Extensive review of cloud based internet of things architecture and current trends," in *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 2021, pp. 1–9.

[21] D. Valtchev and I. Frankov, "Service gateway architecture for a smart home," *IEEE Communications Magazine*, vol. 40, no. 4, pp. 126–132, 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 of Things Journal*, vol. 7, no. 10, pp. 10 102–10 110, 2020.

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

[24] P. Siddhanti, P. M. Asprion, and B. Schneider, "Cybersecurity by design for smart home environments." in *ICEIS (1)*, 2019, pp. 587–595.

[25] Umakant Dinkar Butkar, Dr. Nisarg Gandhewar. (2022). ALGORITHM DESIGN FOR ACCIDENT DETECTION USING THE INTERNET OF THINGS AND GPS MODULE. *Journal of East China University of Science and Technology*, *65*(3), 821–831. Retrieved from http://hdlgdxxb.info/index.php/JE_CUST/article/view/313

[26] Butkar Uamakant, "A Formation of Cloud Data Sharing With Integrity and User Revocation", International Journal Of Engineering And Computer Science, Vol 6, Issue 5, 2017

[27] Umakant Butkar, "IDENTITY BASED CRYPTOGRAPHY WITH OUTSOURCED REVOCATION IN CLOUD COMPUTING FOR FEEDBACK MANAGMENT SYSTEM FOR EDUCATIONAL INSTITUTE", INTERNATINAL JOURNAL OF ADVANCE RESEARCH AND INOVATIVE IDEASIN EDUCATION, vol 2, issue 6, 2016

[28] Umakant Butkar, "A Two Stage Crawler for Efficiently Harvesting Web",International Journal Of Advance Research And Innovative Ideas In Education, Vol 2, Issue 3, 2016

[29] K. Aarika, M. Bouhlal, R. A. Abdelouahid, S. Elfilali, and E. Benlahmar, "Perception layer security in the internet of things," *Procedia Computer Science*, 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 *2018 Second International Conference on Electronics, Com- munication and Aerospace Technology (ICECA)*. IEEE, 2018, pp. 1754–1759.

[31] G. E. Rodr´ıguez, J. G. Torres, P. Flores, and D. E. Benavides, "Cross-site scripting (xss) attacks and mitigation: A survey," *Computer Networks*, vol. 166, p. 106960, 2020.

[32] K. Somasundaram and K. Selvam, "Iot–attacks and chal- lenges," *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 *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*. IEEE, 2020, pp. 346–350.

B. Xu, W. Wang, Q. Hao, Z. Zhang, P. Du, T. Xia, H. Li, and X. Wang, "A security design for the detecting of buffer overflow attacks in iot device," *IEEE Access*, vol. 6, pp. 72 862–72 869, 2018.

[35] E. Dzˇaferovic´, A. Sokol, A. A. Almisreb, and S. M. Norzeli, "Dos and ddos vulnerability of iot: a review," Sustainable Engineering and Innovation, vol. 1, no. 1, pp. 43–48, 2019.

[36] A. Camphouse and L. Ngalamou, "Securing a connected home," in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON), 2019, pp. 0250–0256.

[37] H. Kim and J. Song, “Analysis of iot security in wi-fi 6,” Journal of the Institute of Convergence Signal Processing, 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 Communications and Mobile Computing, vol. 2022, 2022.
[40] F. Zinggeler, “Nokey-a distributed password manager,” Ph.D. dissertation, MS thesis, ETH Zu¨rich, Zu¨rich, Switzerland, 2018.
[41] R. Kishore, U. R. Vigneshwari, N. Prabagarane,
K. Savarimuthu, and S. Radha, “Iot based intelligent control system for smart building,” in 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), 2020, pp. 1–6.
[42] A. Jain, A. Ross, and S. Pankanti, “Biometrics: a tool for infor- mation security,” IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, 2006.
[43] A. Brauchli and D. Li, “A solution based analysis of attack vectors on smart home systems,” in 2015 International Con- ference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 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 Software Engineering, 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,” Telecommunication Systems, vol. 67, no. 3, pp. 423–441, 2018.
[46] T. Jiang, M. Yang, and Y. Zhang, “Research and implementa- tion of m2m smart home and security system,” Security and Communication Networks, vol. 8, no. 16, pp. 2704–2711, 2015.
[47] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Ro- driguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner, and J. Bastos, “A lightweight authentication mechanism for m2m communications in industrial iot environment,” IEEE Internet of Things Journal, vol. 6, no. 1, pp. 288–296, 2019.
[48] S. Thomason, “Improving network security: next generation firewalls and advanced packet inspection devices,” Global Journal of Computer Science and Technology, 2012.
[49] H. Gordon, C. Park, B. Tushir, Y. Liu, and B. Dezfouli, “An efficient sdn architecture for smart home security accelerated by fpga,” in 2021 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN). IEEE, 2021, pp. 1– 3.
[50] M. Bhuyan, S. Kashihara, D. Fall, Y. Taenaka, Y. Kadobayashi et al., “A survey on blockchain, sdn and nfv for the smart-home security,” Internet of Things, p. 100588, 2022.
[51] G. Mantas, D. Lymberopoulos, and N. Komninos, “Security in smart home environment,” in Wireless Technologies for Ambi- ent Assisted Living and Healthcare: Systems and Applications. IGI global, 2011, pp. 170–191.