ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3, March 2022

Security & Privacy Challenges in IoT Based Smart Homes

[1] Naman Chehal *, [2] Karandeep Singh, [3] Supreet Kaur Gill

[1] [2] [3] University College of Engineering , Punjabi University, India

Corresponding Author Email: [1] namanchehal@gmail.com*,[2] karan_rob7@csepup.ac.in, [3] supreetgill13@gmail.com

Abstract*— The Internet of Things (IoT) is a collection of Internet-connected networks, objects, and gadgets. Internally and outwardly, it interacts with the surroundings. The Internet of Things (IoT) detects and reacts to its surroundings. It provides modern approaches to the environment, hence improving mankind's quality of life. IoT enables devices to communicate with one another either in person or online. The Internet of Things (IoT) allows the environment to become smarter and connect with any device at any one time. People nowadays desire to use the Internet to converse with all non-living entities. The Internet of Things (IoT) is used to collect and analyse data from numerous actuators and sensors and then it is analysed before being sent wirelessly to cellphones or computers connection.

Keywords*— Internet of Things (IoT), Smart Homes, Privacy, Security, Threats, Vulnerabilities

I. INTRODUCTION

The Internet of Things (IoT) is a concept that has gained popularity in recent years to describe the connectivity of non-traditional items to the Internet, such as factory machinery, medical equipment, or household appliances. Internet of Things (IoT) interfaces the gadgets, objects through the web utilizing remote innovation. IoT assists with moving, convey, and share the information anyplace whenever through the web. It establishes a far off climate for getting to the information and it has been utilized in some constant applications like savvy urban areas, smart homes, brilliant energy, brilliant farming, savvy industry, and smart residing. IoT has its attributes which incorporate interconnectivity, security, heterogeneity, tremendous scope, dynamic changes, and connectivity. IoT is a mix of a few innovations, for example, Implanted frameworks, inescapable processing, Actuators, Ambient Intelligence, Sensors, Internet Technologies and correspondence advances, and so on. The fundamental aim of IoT is to give simplicity of tasks, remote access control, arrangement, and end-client. IoT gives consistent availability other than the heterogeneous networks. The Internet of Things (IoT) system's primary job is to collect data from the real world and give services to users based on their requests or data processing findings. Cyber entities in the Internet of Things are usually associated with actual items that can be interacted with each other. They work together to fulfil certain tasks. As an example, The Internet of Things (IoT) is an application-driven network that has been used not only in academic research and industry, but also in everyday life, such as smart grids, e-health, e-home, environmental monitoring, smart cities, and so on are only a few examples. In addition, cross-application or cross-domain IoTs are becoming increasingly frequent. Because these IoT based apps are always tied to daily life or work, more and more people are becoming concerned about privacy, while security issues become increasingly complex[1].

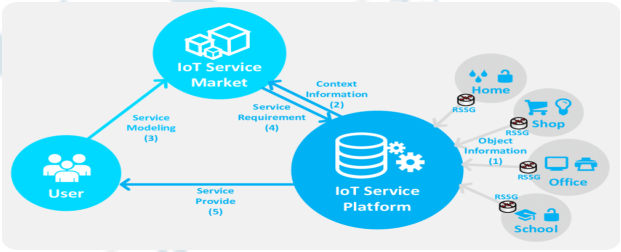

Fig1. An Overview of IoT Environment

II. IoT ARCHITECTURE

We now understand that the Internet of Things is more than just a networked device. In truth, the Internet of Things is a technology that allows systems to sense and respond to their surroundings without the need for human interaction. Because the multiplicity of devices and technology associated with IoT-based systems might be bewildering at times, a generic picture of its architecture merging smart homes and cities should be acknowledged. There is no universally agreed-upon architecture for IoT that the entire world and researchers can agree on. Researchers have proposed a wide variety of architectures. We suggest a broad structure, represented in Figure 2, that incorporates three key layers based on our perspective of IoT-based systems:

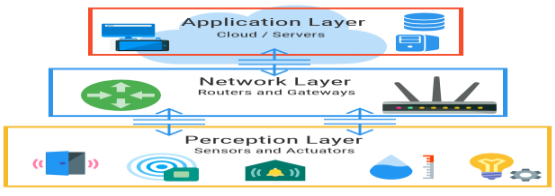

Fig2. The Three Layer IoT Architecture

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3, March 2022

Perception Layer:

A sensor layer is another name for it. It functions similarly to a person's eyes, ears, and nose. It is in charge of identifying objects and gathering information from them. RFID, 2-D barcodes, and sensors are only some of the sorts of sensors that can be attached to things to collect data. The sensors are chosen based on the needs of the applications. These sensors can capture data on location, changes in the air, the surroundings, motion, and vibration, among other things. However, attackers who want to use them to replace the sensor with their own are primarily interested in them. As a result, sensors are the source of the majority of threats [2]–[4]. Common security threats of perception layer are:

Eavesdropping: Eavesdropping is an unlawful real-time attack in which an attacker intercepts private communications such as phone calls, text messages, fax transmissions, or video conferences. It aims to steal data that is being sent via a network. It uses insecure transmission to gain access to the data being sent and received.

Node Capture: Node Capture is one of the most dangerous assaults in the IoT perception layer. A crucial node, such as a gateway node, is taken over by an attacker. It has the potential to leak any data, including communication between sender and receiver, a key used for secure connection, and data kept in memory[5].

Fake Node and Malicious: It's a type of attack in which an attacker adds a node to the system and then injects bogus data into it. Its goal is to prevent the transmission of accurate data. In order to damage the network, an attacker adds a node that uses the energy of actual nodes and potentially controls them.

Replay Attack: It is also known as a play back attack. It's an attack in which an intruder listens in on a conversation between a sender and a recipient and steals the sender's confidential information. By demonstrating confirmation of his identity and authenticity, an intruder delivers the identical validated information to the victim that was already received in his conversation. Because the communication is encrypted, the receiver can treat it as a legitimate request and take the intruder's desired action[6].

Timing Attack: It is usually utilized in gadgets that have feeble figuring abilities. It empowers an aggressor to find weaknesses and concentrate privileged insights kept up with in the security of a framework by seeing how lengthy it takes the framework to react to various questions, input or cryptographic calculations[7].

Network Layer:

Network layer is also known as transmission layer. It serves as a link between the perception and application layers. Through sensors, it carries and communicates the data collected from physical objects. The transmission medium can be wireless or wire-based. It is also in charge of connecting smart items, network devices, and networks to one another. Therefore, it is highly sensitive to attacks from the side of attackers. It poses serious security vulnerabilities with the integrity and authentication of data being transmitted across the network. The following are some of the most common network layer security threats and issues:

Denial of Service (DoS) Attack: A DoS attack is an attack to prevent authentic users from accessing devices or other network resources. It is typically accomplished by flooding the targeted devices or network resources with redundant requests in an order to make it impossible or difficult for some or all authentic users to use them[8].

Main-in-The-Middle (MiTM) Attack: A MiTM attack occurs when an attacker secretly intercepts and modifies communication between a sender and recipient who believe they are interacting directly with each other. Because the attacker has authority over the communication, he or she can change messages to suit their requirements. It poses a significant danger to online security since it allows an attacker to capture and manipulate data in real time[9].

Storage Attack: The information of users is stored on storage devices or the cloud. The attacker can attack both storage devices and the cloud, and the user's information can be modified to erroneous details. Attacks are more likely when information is replicated together with access to other information by different types of persons.

Exploit Attack: Any immoral or unlawful attack in the form of software, chunks of data, or a sequence of commands is referred to as an exploit. It exploits security flaws in an application, system, or piece of hardware. It usually comes with the intention of taking control of the system and stealing data from a network[10].

Application Layer:

Application layer defines all applications that use the IoT technology or in which IoT has deployed. The applications of IoT can be smart homes, smart cities, smart health, animal tracking, etc. It has the responsibility to provide the services to the applications. The services may be varying for each application because services depend on the information that is collected by sensors. There are many issues in the application layer in which security is the key issue. In particular, when IoT is used in order to make a smart home, it introduces many threats and vulnerabilities from the inside and outside. To implement strong security in an IoT based smart home, one of the main issues is that the devices used in smart homes have weak computational power and a low amount of storage for example ZigBee[11].

Common security threats and problem of application layer are:

Cross Site Scripting: It is an injection attack. It empowers an aggressor to embed a client-side content, for example, java script in a believed site saw different clients. By doing so, an attacker can totally change the substance of the application as indicated by his necessities and utilize unique data in an illicit manner[12].

Malicious Code Attack: It is a code in any piece of programming planned to make undesired impacts and harm

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3, March 2022

the framework. A sort of danger may not be hindered or constrained by the utilization of against infection apparatuses. It can either initiate itself or resemble a program requiring a client's regard for play out an activity.

The ability of dealing with Mass Data: Due to a large number of devices and a massive amount of data transmission between users, it has no ability to deal with data processing according to the requirements. As a result, it leads to network disturbance and data loss.

III. MAIN VULNERABILITIES AND THREATS IN SMART HOMES

In a smart home, there is a trade-off between convenience, control, security, and privacy. Smart home components can come in a variety of shapes and sizes, each with its own set of capabilities. Home security, Healthcare, energy, convenience as well as CPU and storage limitations make traditional security solutions for smart home not applicable. There are a few security ideas to keep in mind in this situation in order to provide the most accurate assessment for the smart home risk as well as mitigation[13].

- Assets: Things that are both physical and virtual such as personal information, activities, money and assets are all important to users.
- Threats: Any potential action that might cause damage, harm or loss.
- Vulnerabilities: Weaknesses or gaps inside the system that potentially are exploited by attackers.
- Risk: The potential loss or damage might impact the system by a threat advanced from the system vulnerabilities.

In this segment, we will portray and categorize the main vulnerabilities in the smart home environment. Moreover, the primary threats in the smart home will be introduced and discussed in this section.

Main Vulnerabilities:

According to a study published in[14], 80 percent of IoT devices are vulnerable to a variety of hacks. Adversaries could take advantage of these flaws to manipulate smart home surroundings. The application layer, network layer, and perception layer are the three levels that most IoT systems have[11]. IoT devices are subject to attack and harmful operations at every layer. The most common smart home flaws will be discussed here.

A. Heterogeneous Architecture

To create a smart home system, we'll need a collection of smart home gadgets that work with a range of platforms. The perception layer, network layer, and application layer must all work together to create a dynamic heterogeneous architecture in a smart home. Identifying the nodes that may have access to users' private information due to the heterogeneous architecture of IoT is one of the most common issues in IoT networks[15]. A smart home system is a collection of disparate data, technologies, devices, and protocols. The heterogeneous design of smart devices, along with the dynamic environment of the Internet of Things, forces IoT organisations to device new security measures in order to address new issues[16]. As a result, awareness of how to use IoT apps and systems is critical in order to achieve improved IoT device homogeneity.

B. Outdated Protocols

Some protocols have been outmoded without an upgrade since the Internet's inception, and they can be exploited by attackers[17]. Furthermore, because present devices have limits in terms of integrity, scalability, and compatibility[15] the current security protocols and methodologies are insufficient to address the increasing growth of IoT devices. IoT protocols have weak security capabilities, and trust between these devices is lacking[13]. As a result, new solutions are needed to meet the IoT's privacy, security, and dependability needs.

C. Weak Encryption

Encryption is the process of encrypting data so that only authorised persons can read it, preventing eavesdropping and tampering with data while it is being transmitted. If one piece of data is not encrypted or separated, the data will be transparent, making it easy for attackers to exploit it [15]. Furthermore, some IoT devices employ a tiny encryption key, making them hackable[17]. Because most IoT devices employ different control platforms and protocols, cryptographic solutions to safeguard all IoT systems vary depending on the limits of IoT devices. Sensitive information about a user's daily life is stored in smart home gadgets. Thus, encryption should be at the core of IoT industries as it is an easy and beneficial security method [18].

D. Device Limited and CPU

Smart home gadgets generate a lot of data, which must be computed, evaluated, saved, and processed. Preprocessing of data is usually done at the sensor or at a nearby device[19]. The processing and storage capabilities of IoT devices, on the other hand, are constrained by the resources available, which are severely limited due to computational capability, energy availability, and limited storage[20]. As a result, Denial of Service (DoS) attacks on IoT devices are possible[15].

E. Insecure Applications

IoT applications and middleware systems have not taken into account the lack of systematic ways for building privacy[21]. Some Internet of Things businesses create smart home devices that can be controlled via smartphone apps that are easy to hack. The attackers can simply launch destructive assaults by combining malicious code with applications software deployed on the IoT system[11].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 9, Issue 3, March 2022

F. Poor Authentication

Authentication is the process of providing credentials to a system or entity to verify your identity[13]. Poor confidentiality settings and authentication are the biggest hazards in network communication. Before using IoT devices, change the default credentials because once guessed, they can be used to hack a variety of devices[22]. Inadequate access control of the configuration in the smart home gateway poses the greatest danger of information processing. This danger is mostly due to flaws in the authentication mechanism and insufficient privilege separation across user accounts[23]–[25]

G. Firmware Failure

Many IoT gadgets in the smart home confront a major difficulty since they have no method to upgrade their firmware. Manufacturers rarely consider strategies for confirming firmware integrity during installation, execution, or upgrade because most IoT devices are low-cost[26]. Furthermore, many IoT devices have similar firmware, which increases the chances of successfully exploiting the device, making firmware a major IoT device vulnerability. Because a device's firmware is fixed and never changed, attackers can take advantage of this flaw to start assaults knowing that the virus would function on comparable devices[22].

Main Threats:

To secure any system, it is required to assess the types of risks that may be encountered, as well as how those threats will impact system security. The subsections that follow describe the primary dangers that can affect each layer and have an impact on the smart home environment.

A. Impersonation

In other circumstances, the adversary intends to mimic a legitimate user and act on that user's behalf in order to harm or spy on that user. In order to offer access to IoT devices, social engineering or network traffic eavesdropping can be used to obtain user credentials (user ID and password) [11].

Theft (Identity, credentials, information) The loss of valuable items has a big impact on smart home users. Theft is defined as the taking or use of another person's property without their permission[27]. The attacker attempts to steal valuable authentication and authorization data, such as login passwords or credit card information, from smart-home users. Attackers could employ well-known forms of technology and hardware to get into the smart home and gather information about the user[26].

B. Compromising

The attacker attempts to hack multiple devices and systems, regardless of their identities, in order to profit financially from the information obtained[28]. In addition, an attacker can set up his own node or compromise one of the current ones[29]. Once a network has been breached, the eavesdropper can be hidden within network traffic, making identification extremely difficult. The attacker then begins discreetly employing cyber tools to identify security holes in the network's critical linkages. The malicious software will then scan the smart home infrastructure and probe IoT devices to find system flaws and produce a cyber map of the network's topography. This stage is simple to complete with the help of online tools[28]. Real-time and autonomous interaction between devices make discovering and identifying the compromised nodes very difficult[30].

C. Lack of Encryption

Encryption is a great tool for keeping data safe, but it can be difficult to put into practice on IoT devices. Because many devices lack the processing and storage capacity required for robust encryption, this is the case. As a result, attackers may be able to break encryption keys or modify encryption algorithms.

D. Lack of Physical Hardening

Physical hardening is a critical concern for IoT devices because they are frequently deployed remotely. Without security protections, devices that are exposed to the public can be manually tampered with or stolen. When it comes to physical hardening, it's important to consider how easily recognized and accessible gadgets are. It's also a good idea to turn off any external ports.

E. No Visibility

The scattered nature of IoT devices, along with the possibility of frequent network connections and disconnections, might make them difficult to monitor. You can't notice or respond to suspicious events if you don't have visibility into your devices. As a result, using automated device discovery tools to ensure visibility is crucial.

IV. RECOMMENDED SECURITY SOLUTIONS AND PRACTICES

Many security solutions and practices have been presented in IoT based smart home settings since smart home environments might contain sensitive, important, and private information. Several security solutions for IoT based smart homes have been proposed in the literature in recent years, which are reviewed below.

A. Updating the Software

Updating and upgrading device software, firmware, and firewalls is a critical aspect of keeping security software up to date. A firewall controls traffic between the network and the Internet by acting as a filter between the internet and the interface. Furthermore, the firewall safeguards the network against dangerous software and external threats[31]. In the event of a security breach, the firewall can identify it and give a warning to the user, as well as enact its mitigation method.

To avoid unpatched vulnerabilities, it is also necessary to update the firmware and device software to the most recent version. Out-of-date software still contains the same faults and exploitable vulnerabilities that cybercriminals and hackers can take advantage of. Home automation security vulnerabilities can be mitigated by updating the firewall and device software systems[32].

B. Utilizing Effective Encryption

Wherever possible, the diverse components in an IoT device should encrypt data communication. Encrypted data communication would lessen potential privacy hazards and prohibit unwanted access to data moved between components from benefiting from it. Data that is encrypted is less vulnerable to harmful attacks and illegal access[21].

C. Using Private Network

A secure communication channel is one of the most popular methods used to protect IoT devices from unauthorized access. The secure communication channel can utilize a secure virtual private network (VPN) and limit network traffic such that it is accessible only to authorized users[11].

D. Applying up-to-date Protocols

In order to protect the network, IoT devices must use the most up-to-date protocols. One of the most significant components of IoT is the protocol [17]. It establishes rules for establishing consistent communications between devices. As a result, in order to regulate, interact, and exchange data, embedded computer services require a set of rules[13].

E. Changing Credentials Regularly

IoT manufacturers should require users to update their default identities (username and password) to strong ones the first time they use an IoT device, unless the IoT device should not be used. Furthermore, the password should be changed at least once every three months. Furthermore, users should create separate passwords for different IoT devices rather than using the same password for all of them. Furthermore, it is strongly advised against using the email address as a username, as this is a typical tactic used by attackers to phish email accounts and steal passwords [33].

F. Backup Significant Information

Some smart home gadgets, such as healthcare devices, include sensitive information that can only be accessed by authorized individuals. Backing up such data on a regular basis is the greatest approach to protect it from forgery or theft. The research study in [11] provides advice for backing up sensitive data, such as media data, and storing it off site, either digitally or physically.

G. Monitoring the Network

Monitoring the connectivity of IoT devices during message transfer is one of the recommended practices for securing smart homes. Microsoft Message Analyzer is one of many tools that can help you monitor your network and analyze device messages. Furthermore, the monitoring software may look for flaws in IoT programs and subsequently update them.

V. CONCLUSION

IoT devices and applications are playing an essential role in our modern life. With the Internet of Things, every physical object will be a digital device, collecting information and conducting computing the Internet connectivity. We can see IoT devices almost everywhere from our homes, offices, shopping centers, schools, airports, and many other places to provide us with secure and on-demand services. Integration of IoT devices in the home environment has tremendously increased in recent years, with the goal of improving the quality of our lives at home by making them easier, more pleasant, and convenient. Privacy and security in IoT contexts, on the other hand, have been cited as important impediments to the smart home. The architecture, threats, and security of smart home environments were all discussed in this research. Analyzed possible security attacks that may be critical in the development and implementation of IoT in different areas and classified with respect to layers of IoT architecture: perception layer, network layer and application layer. More importantly, the most frequent smart home threats and vulnerabilities were described and discussed. Finally, this article outlined the best user practices and suggested solutions for smart home environments.

REFERENCES

[1] X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," *Digital Communications and Networks*, vol. 7, no. 3. Chongqing University of Posts and Telecommunications, pp. 373–384, Aug. 01, 2021, doi: 10.1016/j.dcan.2020.09.001.

[2] H. Suo, J. Wan, C. Zou, J. L.-2012 international conference on, and undefined 2012, "Security in the internet of things: a review," *ieeexplore.ieee.org*, 2012, doi: 10.1109/ICCSEE.2012.373.

[3] D. Kozlov, J. Veijalainen, Y. A.- BODYNETS, and undefined 2012, "Security and privacy threats in IoT architectures.," *researchgate.net*, 2012, doi: 10.4108/icst.bodynets.2012.250550.

[4] X. X.-2013 I. conference on computational and undefined 2013, "Study on security problems and key technologies of the internet of things," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022.

[5] M. Bharathi, … R. T.-2012 I., and undefined 2012, "Node capture attack in Wireless Sensor Network: A survey," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022. [Online].

[6] D. Puthal, S. Nepal, R. Ranjan, J. C.-I. C. Computing, and undefined 2016, "Threats to networking cloud and edge datacenters in the Internet of Things," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022.

[7] D. Brumley, D. B.-C. Networks, and undefined 2005, "Remote timing attacks are practical," *Elsevier*, Accessed: Feb. 17, 2022. [Online].

[8] "Prabhakar: Network security in digitalization: attacks... - Google Scholar."

[9] M. Conti, N. Dragoni, & V. L.-I. C. S., and undefined 2016, "A survey of man in the middle attacks," *ieeexplore.ieee.org*, Accessed: Feb. 17, 2022. [Online].

[10] "What is computer exploit? - Definition from WhatIs.com."

[11] B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," *Sensors (Switzerland)*, vol. 18, no. 3, pp. 1–17, 2018, doi: 10.3390/s18030817.

[12] S. Gupta, … B. G.-J. of S. A. E. and, and undefined 2017, "Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art," *Springer*, Accessed: Feb. 17, 2022. [Online].

[13] D. Bastos, M. Shackleton, and F. El-Moussa, "Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments," 2018.

[14] "Smart Home: Threats and Countermeasures - Rambus."

[15] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2019, doi: 10.1109/JIOT.2018.2869847.

[16] D. E. Kouicem, A. Bouabdallah, H. Lakhlef, D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security : A top-down survey To cite this version : HAL Id : hal-01780365 Internet of Things Security : a top-down survey," 2018.

[17] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh, "Security vulnerabilities in bluetooth technology as used in IoT," *J. Sens. Actuator Networks*, vol. 7, no. 3, pp. 1–26, 2018, doi: 10.3390/jsan7030028.

[18] "How Encryption is Powering the Future of IoT." https://www.iotforall.com/future-iot-encryption (accessed Feb. 24, 2022).

[19] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.

[20] S. Milivojevic, "'The Internet of Everything,'" *Crime Punishm. Futur. Internet*, vol. 7, no. 1, pp. 60–79, 2021, doi: 10.4324/9781003031215-4-4.

[21] C. Perera, C. McCormick, A. K. Bandara, B. A. Price, and B. Nuseibeh, "Privacy-by-design framework for assessing internet of things applications and platforms," *ACM Int. Conf. Proceeding Ser.*, vol. 07-09-Nove, pp. 83–92, 2016, doi: 10.1145/2991561.2991566.

[22] "(PDF) Internet Of Things (Iot) Security Best Practices. IEEE Community-led White Paper | Jared Bielby, rajesh nighot, and Sukanya Mandal - Academia.edu." https://www.academia.edu/32053241/Internet_Of_Things_Iot_Security_Best_Practices._IEEE_Community-led_White_Paper (accessed Feb. 24, 2022).

[23] "Cisco 2017 Annual Cybersecurity Report | The Network.".

[24] "(PDF) A risk analysis of a smart home automation system | Ramakrishna Bhat - Academia.edu." https://www.academia.edu/29318863/A_risk_analysis_of_a_smart_home_automation_system (accessed Feb. 24, 2022).

[25] A. A. Ahmed and W. A. Ahmed, "An effective multifactor authentication mechanism based on combiners of hash function over internet of things," *Sensors (Switzerland)*, vol. 19, no. 17, 2019, doi: 10.3390/s19173663.

[26] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, and G. Baldini, "Security and privacy issues for an IoT based smart home," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, no. 1, pp. 1292–1297, 2017, doi: 10.23919/MIPRO.2017.7973622.

[27] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, 2018, doi: 10.1016/j.cose.2017.10.008.

[28] I. G. Seissa, J. Ibrahim, and N. Yahaya, "Cyberterrorism Definition Patterns and Mitigation Strategies: A Literature Review," *Int. J. Sci. Res.*, vol. 6, no. 1, pp. 180–186, 2017, doi: 10.21275/art20163936.

[29] H. Rahmani, N. Sahli, and F. Kamoun, "Distributed denial-of-service attack detection scheme-based joint-entropy," *Secur. Commun. Networks*, vol. 5, no. 9, pp. 1049–1061, 2012, doi: 10.1002/sec.392.

[30] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018, doi: 10.1016/j.future.2017.07.060.

[31] N. Apthorpe, D. Reisman, S. Sundaresan, A. Narayanan, and N. Feamster, "Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic," 2017

[32] S. Ur Rehman and V. Gruhn, "An approach to secure smart homes in cyber-physical systems/Internet-of-Things," *2018 5th Int. Conf. Softw. Defin. Syst. SDS 2018*, pp. 126–129, 2018, doi: 10.1109/SDS.2018.8370433.

[33] "Best Practices for Security within the Internet of Things."