SECURITY ATTACKS AND COUNTERMEASURES IN SMART HOMES

Hasibul Alam and Emmett Tomai

Department of Computer Science, The University of Texas Rio Grande Valley, Texas, USA

ABSTRACT

The Internet of Things (IoT) application is visible in all aspects of humans' day-to-day affairs. The demand for IoT is growing at an unprecedented rate, from wearable wristwatches to autopilot cars. The smart home has also seen significant advancements to improve the quality of lifestyle. However, the security and privacy of IoT devices have become primary concerns as data is shared among intelligent devices and over the internet in a smart home network. There are several attacks - node capturing attack, sniffing attack, malware attack, boot phase attack, etc., which are conducted by adversaries to breach the security of smart homes. The security breach has a negative impact on the tenants' privacy and prevents the availability of smart home services. This article presents smart homes' most common security attacks and mitigation techniques.

KEYWORDS

Internet-of-Things, Smart Home Architecture, Security Attacks on Smart Homes, Application of Smart Homes

1. INTRODUCTION

The Internet of Things (IoT) refers to connecting devices – "things"– that are integrated with software, sensors, and other technologies capable of connecting to the internet and other smart devices. IoT has rapidly expanded over the past several years, revolutionizing our lifestyle and interaction with different devices. Several application areas, including transportation, smart homes, energy, agriculture, healthcare, manufacturing, and many more, are being significantly impacted by IoT. According to Statista, there will 29.42 billion be connected smart devices by 2030 [1]. In addition, the International Data Corporation has also predicted that IoT devices will generate 80 Zeta Byte data by 2025 [2]. By the end of 2022, it is anticipated that the smart home market would be worth $222.90 billion [1].

A smart home (SH) interconnects heterogeneous devices on top of an IoT platform. The smart items in smart home infrastructure interact with each other through a gateway using distinct wireless network protocols. Due to insecure protocols and the reduced processing capability of smart devices to embrace advanced security features, smart home is prone to security attacks [3]. Correspondingly, IoT devices in smart homes may compromise with evildoers who observe the activity of inhabitants and steal personal information. An SH environment is susceptible to several security threats, including data privacy, authorization, authentication, issues with access control, and system configuration. Denial of Service attacks, Malware attacks, Hard-coded password attacks, Eavesdropping attacks, etc., are the most common attacks conducted in a smart home. These attacks cause inconveniences in smart home users' lifestyles and privacy. For example, adult children in the USA, Europe, or Japan do not live with elderly parents. They can

David C. Wyld et al. (Eds): DBML, CITE, IOTBC, EDUPAN, NLPAI -2023
pp.109-119, 2023. IJCI – 2023 DOI:10.5121/ijci.2023.120209

use the smart camera to monitor their parents and send messages to do physical exercise, take medicine, etc. Attackers can use the smart camera to verify if tenants are present in the house or collect visual data about the tenants.

Security measures have been proposed to overcome the security concerns for the prevalent attacks on smart homes. In this article, First, we present the architecture of the smart home. Second, point out the major applications of the smart home. Lastly, we present the security attacks along with countermeasures.

The rest of the article is outlined as follow. A summary of the fundamental concepts of smart home is given in Section 2. The applications of smart homes are highlighted in Section 3. Section 4 presents security attacks on smart homes and highlights the mitigation techniques of the security attacks.

2. OVERVIEW ON SMART HOME SYSTEM

An SH is an IoT application that enables end users to remotely monitor and manage household appliances in real time. Smart technologies have permeated every corner of human's everyday lives in the modern age, including lights, smartphones, thermostats, washing machines, refrigerators, smart TVs, smart sensors, etc. These intelligent gadgets interact and communicate with each other to create an intelligent environment, as shown in Figure 1. When given access to the Internet, such an automation system transforms into an IoT-based smart home system [4].

2.1. Smart Home Architecture

A smart home ecosystem is a three-layered architecture: device layer, controller layer, and cloud service/storage layer, which is demonstrated in Figure 1.

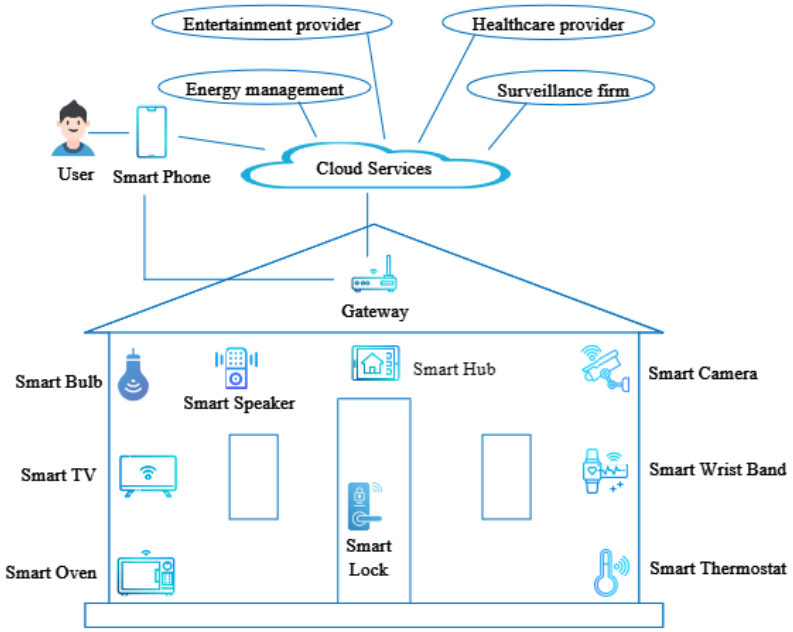

Figure 1. Generic smart home architecture

2.1.1. Device Layer

This layer is in charge of keeping an eye on the environment and gathering information. Since it works with the actual world, it must be developed using real-world objects kept in a home. The smart home device layer is composed of hardware consisting of sensors, actuators, and smart things.

Sensors - Sensors can extract the characteristics of their surroundings and turn them into a digital output which is then analysed by the system to identify the current status of the environment. Various sensors are used in smart home environments, such as temperature, motion, contact, etc.
Actuators - Actuators have manipulation and control capability over the physical environment. It receives digital signals from the system that is then translated into actions - turning on/off lights, triggering alarms, activating speakers, etc.

Smart Things - Smart things are objects with sensors and actuators connected to the smart home network. Examples of smart things include objects like a smart bulb that switches on based on motion detection, a smart lock, a smart camera, etc.

2.1.2. Controller Layer

The controller layer functions as a central decision-making structure that collects and correlates data from smart home devices. It makes decisions and initiates actions by sending messages and commands to the relevant devices based on the information received or the situation [5]. The controller can be a device (e.g., Alexa, Google Home, Xiaomi smart speaker, etc.) or a cloud application. Several smart home devices available in the market, such as Apple's HomeKit, Google Nest Weave, Samsung's SmartThings, Alibaba Smart Living, etc., are controlled by a compatible Intelligent Virtual Assistant (IVA) or application installed in a smartphone or computer. Though most smart devices have the processing capacity and act like independent or autonomous devices (e.g., smart thermostats, smart TV, etc.), they somehow require an interface between them and the cloud or user. In that case, an application or IVA functions as an interface part of the controller layer [6].

2.1.3. Cloud Service/Storage Layer

This layer stores sensor or device-generated data providers use to facilitate smart home users with specialized services. Services are applications hosted in the cloud that the user uses to control or manage the device. Hosted applications are responsible for collecting data, processing data, analysing data, decision-making, etc.

3. SMART HOME APPLICATIONS

There are several smart home applications or services. Presenting four major categories - Entertainment & comfort, Healthcare, Surveillance, and Energy management with use case scenarios. Table 1 shows key services included in each category.

Table 1. Categories of Smart Home Applications

Entertainment & Comfort	Healthcare	Surveillance	Energy management
Simple to utilize and regulate	Befitting tenant housing, especially elderly	Identifying strangers	Ensuring efficient energy usage
Offer comfort	Continuous patient monitoring	Detecting movement of objects	Logical usage of gadgets
Reduce physical interaction with devices	Precautionary treatment warning	Preventing unfortunate incidents	Reliability and quality of devices
–	Easy interaction with medical institutes	–	–

3.1. Entertainment & Comfort

Smart home optimizes their users' lifestyle through programmable devices or can be managed remotely using software programs. Thus, it improves the comfort, convenience, and interactivity of smart home users [7]. For example, smart lights automatically turn off when inhabitants of the home leave and turn on when it detects the movements of inhabitants by a motion sensor. Smart watering is also another example of a programmed or scheduled system that opens all the conduits when a certain time is met for watering plants. Intelligent personal assistants are voice-controlled, hands-free gadgets that can perform various tasks, including voice communication, internet surfing, playing videos/audio, and managing other devices - smart thermostats, smart bulbs, etc. [6]. Apple Siri, Google Assistant, Microsoft Cortana, and Amazon Alexa are the most popular and commonly used intelligent personal assistants.

3.2. Healthcare

Healthcare services for inhabitants of smart homes have seen a revolutionary improvement, especially for elderly persons with disabilities. Different sensors and smart gadgets can be installed in a smart home to look for physical or mental abnormalities of the occupants. This prospect offers various advantages, including reduced expenses in contrast to institutional living, giving elderly people an opportunity to stay with their families instead of living alone in a healthcare institution. For example, smart speakers and screens inform the patient or elderly person which medicine to take and other tasks [8].

3.3. Surveillance

Several features of smart devices can be used for surveillance and security of smart homes. For instance, intrusion detection can be accomplished by using motion sensors and smart cameras. If the movement of an unknown person is detected, an intrusion detection application will trigger a message to the homeowner; even the system can send an audio/video message, including the person's image. Smart surveillance cameras take advantage of image classification techniques to identify unknown people. Smart door locks with cameras can be used to give entry permission to privileged people [9].

3.4. Energy Management

Smart things are utilized in smart homes to deliver cutting-edge technology and save energy consumption. For instance, the smart lighting system can properly utilize self-generated energy in the daytime. At the same time, it can save energy conservation at night by shutting off all the

standby devices [10]. A smart grid provides efficient power supply and consumption using information technology and grid energy systems [5]. A smart meter can be integrated into the home to track energy consumption patterns. The system automatically sends energy consumption reports to users and vendors. Based on the report, the vendor can provide recommendations to reduce energy usage [11].

4. SECURITY ATTACKS ON SMART HOMES

Passive attacks and active attacks are the two types of security attacks that can be conducted against smart homes. Passive assaults aim to watch without affecting data or network performance. These attacks are typically imperceptible and use transmissions, eavesdropping, and monitoring techniques to operate. In active attacks, the attackers use the data obtained by passive attacks to alter the data, messages, system operations, or system resources. Malware, message modification, password cracking, and denial-of-service attacks are typical active attacks. To mitigate or neutralize these attacks researcher recommended various mechanisms. Table 2 shows the security attacks and mitigation techniques discussed in this paper.

4.1. Node Capturing

Attackers can readily target these frail sensors since the smart home network consists of numerous devices and low-power sensors. Attackers swap out existing network nodes with their personal one to gather information. These rogue nodes pose as reliable devices while serving the interests of attackers [12]. As mentioned by Gavra *et al.,* [13] attackers have full control of the sensors and operate them, but physical sensors are in the system. It's a threat for the smart home network unless the rogue device gets identified. To get rid of this attack, mitigations section discusses the befitting techniques.

Mitigation - If smart devices are compromised or disconnected from their network, the node-capturing attack can be minimized by wiping key information and data from memory. This can be accomplished by embedding a special chipset in IoT. The market has chipsets such as MAX36010 and MAX36011 (chipsets by Maxim Integrated) that can erase secure memory. Therefore, developing chipsets adaptable to IoT can solve the issue. Node tampering also can be mitigated by integrating anti-counterfeit hardware primitives such as Physically Unclonable Function (PUF) that trigger a unique response for a challenge input [14]. Thus, a PUF installed on a smart device can identify and protect against node capture attacks.

Table 2. Security attacks and mitigations

Security Attack	**Mitigation Technique**
Node capturing	Embedding special chipset, Integrating Physical Unclonable Function [14]
Boot phase attack	Cryptographic code signing technique [16]
Sniffing attack	Trustworthy network with authentication measures and encryption protocols
Eavesdropping	Lightweight and portable encryption methods [18] [14]
Hard-coded/Default password	Modifying default password with some complexity, One Time Password, Transport Layer Security [19] [20] [21]
Distributed Denial of Service attack	Lightweight DDOS mitigation system, Machine learning algorithms [22], Blockchain network [23]
Malware attack	Whitelisting-based solution [24], Blockchain-based autonomous system [25]

4.2. Boot Phase Attack

Built-in security features are inoperative during the boot phase in smart objects. Devices become susceptible to different security threats throughout this procedure. Due to this flaw, attackers use the gadgets as a target for their evil intentions, like inserting malicious firmware code. As a result, making smart devices resistant to booting process vulnerabilities is crucial [15]. Attackers can carry out their tasks even while devices are not currently in communication mode by using physical communication protocols like UART or JTAG [13].

Mitigation - Cryptographic code signing techniques can be implemented to protect smart devices against boot-phase attacks. The code executed on the device can be created by the device's manufacturer or a reliable vendor. This approach can lessen the likelihood of replication of firmware code by the attacker [16].

4.3. Sniffing Attack

Attackers gather users' confidential information by placing malicious devices or sensors instead of actual devices. They infiltrate the system as sniffer programs and run them to steal private data while users are unaware of the exploitation [17].

Mitigation - It is crucial to make sure that devices are connected to a secure network with proper authentication mechanisms in order to prevent sniffing. In addition to that, as attackers track the network traffic to find users' credentials to conduct sniffing, encryption protocols such as AES, RSA, Triple DES, etc., should be applied to encrypt the data which leaves smart devices so that the original information is not understandable to adversaries [16].

4.4. Eavesdropping

In this attack, attackers eavesdrop on the network communication to monitor or steal the data without any alteration. It is very straightforward to conduct eavesdropping as the smart devices and servers in smart homes communicate via the internet. Due to the different technological limitations of smart home things, traditional encryption mechanisms cannot always be used [6]. Utilizing this scope, adversaries can access sensitive data such as banking information (e.g., credit card numbers, expiration date, CVC, etc.), camera video recordings while sending to the storage, etc.

Mitigation - Typically, IoT devices cannot use traditional data encryption algorithms due to memory limitation and processing capacity. To address the requirements, Thakor *et al.,* [26] suggested the best suit algorithms such as SIMON, SPECK, PICCOLO, TWINE, PRESENT, and Midori for smart home devices like smart refrigerators, smart bulbs, health care appliances, etc. based on real-time use case studies. Lata and Kumar [18] also suggested some lightweight stream ciphers - Espresso, ChaCha, Grain, Trivium, etc. that fit the demanding requirements. To prevent adversaries from eavesdropping, Tejasvi *et al.,* [14] proposed to set up low-cost demilitarized zones at the user's end as buffer zones.

4.5. Hard-coded/Default Password

When users purchase IoT devices, they typically come with hard-coded or default credentials in the guise of a username and password. Hard-coded credentials cannot be changed even if users want to do so, while users can modify default credentials according to credential definitions and rules. The default credentials are frequently available on the vendors' websites or are easy to guess. Due to the lack of awareness of cybersecurity issues, users do not modify the default credentials. Attackers can utilize the opportunity to gain illegal access to smart devices and smart

home network and conduct various attacks such as access to IoT shell service, data identity theft, social engineering, etc. Like every year, according to SplashData, the worst password of 2022 is `123456' [27]. NordPass also listed the password as the most used one with 103,170,552 counts, and it takes less than a second to crack it [28].

Mitigation - There are several sophisticated authentication techniques available today that are based on trustworthy and secure cryptographic algorithms [29] [30], including those that use One Time Password (OTP) [21], Datagram Transport Layer Security (DTLS), and Transport Layer Security (TLS) that has been adapted for the Internet of Things (IoT) [19] [20]. Modifying the default passwords with some complexity is the least effort to mitigate this attack.

4.6. Distributed Denial of Service (DDoS)

Adversaries conduct a DDoS attack to disrupt or delay services temporarily or indefinitely to legitimate users [31]. In the context of Smart Home, a group of compromised devices scattered over the internet called a botnet is utilized to operate a DDoS attack against a target device or network shown in Figure 2. And a single compromised device is used to conduct a Denial of Service (DoS) attack against a victim device. To successfully operate the attack, attackers launch several techniques, such as flooding with requests or responses to exceed the bandwidth of the victim system (UDP Floods, ICMP Floods), exploiting protocol flaws (SYN Floods, Ping of Death), or flooding a victim device with service requests out of its capacity to respond. A flooding attack is the most dangerous and popular attack among attackers as it is very effective against any service and easy to initiate [32]. Launching a flood attack, adversaries do not require protocols flaw or identification of devices but flood the targets [33], as the Internet of Things has limited memory and processing capacity. DDoS/DoS attack in the smart home system has different consequences, such as targeting a smart refrigerator causing food waste is different than the consequence of neutralizing a motion sensor that detects movement in a room. The effect of targeting a health service can have a disastrous impact on patient health while targeting a smart grid meter that causes a power shutdown. The most alarming thing is the mentioned attack has the potential to bring down the entire system targeting the C&C unit or all the services that rely on the internet targeting system gateway.

Mitigation - Although DDoS attacks are highly challenging to identify and stop, there are strategies to lessen their effects. Yaegashi *et al.,* [34] presented a lightweight DDoS mitigation system on the edge of the IoT network that makes use of the restricted capabilities of low-cost devices like a smart home gateway to recognize and mitigate flood assaults. In attacks like UDP flood, the mitigation system uses vacant queue resources to identify malicious traffic flows by randomly shuffling queue distribution and dropping packets from recognized flows. Machine learning algorithms can detect DDoS attacks by filtering out the packets based on the user parameters and packet attributes from the flowing traffic packets in the network. Hasan *et al.,* [22] introduced a machine learning approach to predict DDoS attacks in IoT sensors using Artificial Neural Network (ANN), Support Vector Machine (SVM), and Logistic regression (LR) models. Selecting the number of traffic attributes as minimum as possible makes this cost-effective approach [35]. Although this approach also can be used to mitigate Mirai (a DDoS variant), it is not very effective in changing the obfuscation [36]. The authors in [23] [37] presented the distributed architecture-based solution called Blockchain as redundant data storage in which network nodes keep a record of transactions in a digital ledger. It is highly challenging to launch a DDoS assault or flooding attack on every node of a blockchain network since the total number of transactions that can be processed at one time is constrained.

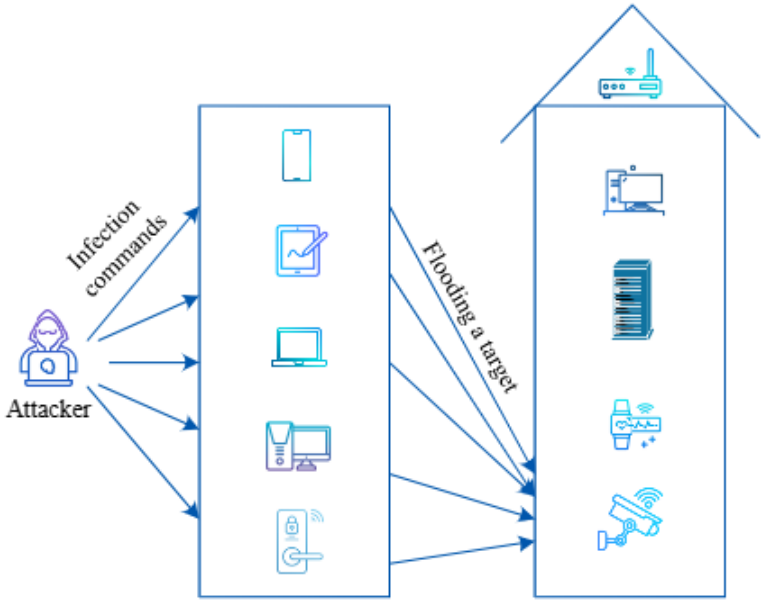

Figure 2. DDoS attack procedure

4.7. Malware Attack

With the passage of time, adversaries are showing more interest in malware attacks on IoT devices. Popular malware attacks such as Bashlite, Silex, and Mirai are conducted on smart home devices and IoT. Bashlite, the predecessor of Mirai, operates using default or weak credentials on IoT devices, especially by exploiting Apache Struts vulnerability [38]. On the other hand, Mirai is more complicated than Bashlite though it utilizes default login information to attempt brute-force attacks on vulnerable devices and include them in the botnet. To carry out the attack, compromised devices look for more vulnerable devices nearby by finding open Transport Control Protocol ports or IP addresses. Once a port is found, it conducts a brute-force attack using a dictionary of IoT devices' 62 most common user credentials. When a brute-force assault is successful, the compromised device receives an administrative shell, and the C&C server receives a report. Then the bot-master issues an in-fact command whose payload includes an IP address and hardware architecture. The compromised device's binary malware version is downloaded and executed when the payload logs in and issues the appropriate instructions. In 2018, Mirai was used to perform the greatest DDoS assault human know of which has a throughput of over 1.7 TB/s [39]. Another malware that targets IoT devices and operates on the Internet is Silex, which concentrates on Unix-based devices. To render a device unusable to users, Silex traces a susceptible device, corrupt the system memory with random data, clears out network configuration, and then reboots the device [40]. Silex compromised up to 4,000 susceptible IoT devices before the author shut it down.

Mitigation - T. S. Gopal *et al.*, [41] proposed a whitelisting-based solution preventing malware from spreading in IoT. The solution works in two phases. On a clean device, the profiling module creates a hash for all the programs running on the IoT devices and router in the first phase and preserves it in the database. In the second phase, the application whitelisting is conducted by the "Application Monitor" computing hash of the application before its execution and comparing it with the stored hash in the database. The program is trusted and executed if the outcome is affirmative; otherwise, it is marked as unsafe and banned. In the paper [24], authors proposed a mitigation approach that focuses on the network architecture of smart homes and the effective

arrangement of a worm called Hajime that has no capability to conduct a DDoS attack. They considered star and tree topologies for network structure and placed Hajime in the centre while considering the Mirai attack from the edge of the network. It shows that the tree topology of the IoT network performs better in terms of the rate of Mirai infection as devices are grouped in different subnets. Z. Ahmed *et al.*, [25] presented a blockchain-based architecture to prevent Mirai attacks on IoT devices where the network is partitioned into different Autonomous Systems (AS), through which host connectivity is achieved. A list of IP addresses for various hosts linked to an AS, together with an indication of which has been deemed malicious, are stored, and shared using blockchain. Each AS keeps track of communication activity within the network and decides if a host is compromised by comparing the total number of packets delivered by the host with a predetermined threshold value.

5. CONCLUSION

People have hastened the use of smart gadgets in their everyday lives and have quickly got used to smart homes because they offer a broad variety of applications. Due to the mass use of smart devices, the security and privacy of smart homes have become crucial. Befitting countermeasures for the security attacks - node capturing, sniffing, DDoS, malware attack, etc., have been presented in this paper. Each Mitigation technique functions alone without collaborating with other techniques, making it difficult to manage the smart home system. As a future work, it would be better to find a countermeasure that can counter multiple security concerns or provide a framework that can implement multiple mitigation techniques, if not all. To carry out this idea, blockchain technology can be a viable option as blockchain itself is a security measure, though implementing blockchain in resource constant IoT devices will be a challenging task. Fine-tuning the existing blockchain technologies according to IoT devices' requirements or proposing a noble lightweight blockchain can be a way forward.

REFERENCES

[1] "Number of internet of things (iot) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030," Available at https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (2022/08/22).

[2] "Future of industry ecosystems: Shared data and insights," Available at https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/ (2022/08/22).

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *ArXiv*, vol. abs/1608.05187, 2016.

[4] C. Yang, E. Mistretta, S. Chaychian, and J. Siau, "Smart home system network architecture," pp. 174–183, 2016.

[5] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production,* vol. 140, pp. 1454–1464, 2017.

[6] B. Hammi, S. Zeadally, R. Khatoun, and J. Nebhen, "Survey on smart homes: Vulnerabilities, risks, and countermeasures," *Computers Security*, vol. 117, p. 102677, 2022.

[7] M. Mahnoosh, B. Srinivas, and S. Benjamin, "Personalized speech recognition for internet of things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, 2015, pp. 369–374.

[8] K. Murad, D. Sadia, J. Sohail, G. Moneeb, G. Hemant, and M. SC, "Context-aware low power intelligent smarthome based on the internet of things," *Computers & Electrical Engineering*, vol. 52, pp.208–222, 2016.

[9] L. Changmin, Z. Luca, C. Kwanghee, and C. Hyeong-Ah, "Securing smart home: Technologies, security challenges, and security requirements," in *2014 IEEE Conference on Communications and Network Security*, 2014, pp. 67–72.

[10] F. Roy and H. Gerhard, "Dtls for lightweight secure data streaming in the internet of things," in *2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing. IEEE*, 2014, pp. 585–590.

[11] K. Nikos, P. Eleni, and P. Andreas, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, 2014.

[12] K. S. Kumar, S. R. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, "Security enhancements to system on chip devices for iot perception layer," *2017 IEEE International Symposium on Nanoelectronics and Information Systems (iNIS)*, pp. 151–156, 2017.

[13] G. V. Dacian, D. I. Marian, and P. O. Aurel, "A survey on threats and security solutions for iot," in *20204 3rd International Spring Seminar on Electronics Technology (ISSE)*, 2020, pp. 1–5.

[14] A. Tejasvi, C. Vinay, S. Biplab, and C. K.-K. Raymond, "Consumeriot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[15] H. Vikas, C. Vinay, S. Vikas, J. Divyansh, G. Pranav, and S. Biplab,"A survey on iot security: Application areas, security threats, andsolution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[16] T. Haseeb, Z. Shakir, A. Rashid, H. Mudassar, A.-T. Fadi, andB. Muhammad, "Smart home security: challenges, issues and solutions at different iot layers," *The Journal of Supercomputing*, vol. 77,no. 12, pp. 14 053–14 089, 2021.

[17] V. Shivangi, R. Jyotsnamayee, M. Janit, V. Saurav, and P. Chetana,"Internet of things (iot): A vision, architectural elements, and securityissues," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2017, pp. 492–496.

[18] L. Navdeep and K. Raman, "Analysis of lightweight cryptography algorithms for iot communication," in *Congress on Intelligent Systems*. Singapore: Springer Singapore, 2021, pp. 397–406.

[19] R. T. Tiburski, L. A. Amaral, E. de Matos, D. F. G. de Azevedo, and F. Hessel, "Evaluating the use of tls and dtls protocols in iotmiddleware systems applied to e-health," *2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 480–485, 2017.

[20] Urien and Pascal, "Innovative tls/dtls security modules for iot applications: Concepts and experiments," in *Internet of Things. IoT Infrastructures*, 2016, pp. 3–15.

[21] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ecc-based authentication scheme for internet of things (iot)," *IEEE Systems Journal*, vol. 14, pp. 3440–3450, 2020.

[22] H. Mahmudul, I. M. Milon, Z. M. I. Islam, and H. MMA, "Attack andanomaly detection in iot sensors in iot sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019.

[23] W. Ziyan, D. Xinghua, L. Yi, F. Li, and C. Ping, "Iot security model and performance evaluation: A blockchain approach," in *2018 international conference on network infrastructure and digital content (ic-nidc)*, 2018, pp. 260–264.

[24] T. Hiroaki, Y. Shingo, and A. Takuya, "Consideration of iot structure in mitigation against miraimalware," in *2018 IEEE 8th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, 2018, pp. 1–3

[25] A. Zohaib, D. S. Muhammad, Q. H. Khaliq, and L. Marios, "Protecting iots from mirai botnet attacks using blockchains," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[26] T. V. A., R. M. Abdur, and K. M. R. A., "Lightweight cryptography algorithms for resource-constrained iot devices: A review, comparison and research opportunities," *IEEE Access*, vol. 9, pp. 28 177–28 193, 2021.

[27] "100 most common passwords of 2022. can you spot your password?" Available at https://techcult.com/most-common-passwords/(2022/10/18).

[28] "Top 200 most common passwords," Available at https://nordpass.com/most-common-passwords-list/ (2022/10/18).

[29] E. hajj Mohammed, F. Ahmad, C. Maroun, and S. Ahmed, "A survey of internet of things (iot) authentication schemes," *Sensors*, vol. 19, no. 5, 2019.

[30] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for internet of things," *Internet of Things*, vol. 14, p. 100075, 2021.

[31] A. C, M. H, and O. A, "Defense for distributed denial of service attacks in cloud computing. Tunisia," 2015.

[32] B. Hammi, D. Guillaume, and K. Rida, "Toward a source detection of botclouds: A pca-based approach," in *Monitoring and Securing Virtualized Networks and Services*, 2014, pp. 105–117

[33] B. Hammi, D. Guillaume, and K. Rida, "Understanding Bot clouds from a system perspective: A principal component analysis," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, 2014, pp. 1–9.
[34] Y. Ryo, H. Daisuke, and N. Yu, "Light-weight ddos mitigation at network edge with limited resources," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, 2021, pp.1–6.
[35] M. Sudip, K. P. Venkata, A. Harshit, S. Antriksh, and O. M. S, "A learning automata-based solution for preventing distributed denial of service in internet of things," *in 2011 international conference on internet of things and 4th international conference on cyber, physical and social computing,* 2011, pp. 114–122.
[36] S. Jiawei, V. D. Vargas, P. Sanjiva, S. Daniele, F. Yaokai, and S. Kouichi, "Lightweight classification of iot malware based on image recognition," in *2018 IEEE 42Nd annual computer software and applications conference (COMPSAC)*, vol. 2, 2018, pp. 664–669.
[37] S. Georgios, G. Nikolaos, D. Georgios-Paraskevas, and T. Georgios,"Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets," *Future Internet*, vol. 11, no. 11, p. 226, 2019.
[38] C. Osborne, "Mirai, gafgyt iot botnets stab systems with apache struts, sonicwall exploits." [Online]. Available: https://www.bit.ly/3kcs8mc
[39] Y. Seralathan, T. T. Oh, S. Jadhav, J. Myers, J. P. Jeong, Y. H. Kim, and J. N. Kim, "Iot security vulnerability: A case study of a web camera," *2018 20th International Conference on Advanced Communication Technology (ICACT)*, pp. 172–177, 2018.
[40] L. O'Donnell, "Thousands of iot devices bricked by silex malware." [Online]. Available: https://threatpost.com/thousands-of-iot-devices-bricked-bysilex-malware/ 146065/,June2019
[41] T. S. Gopal, M. Mallesh, J. G, P. R. L. Eswari, and E. Magesh, "Mitigating mirai malware spreading in iot environment," in *2018 International Conference on Advances in Computing, communications, and Informatics (ICACCI)*, 2018, pp. 2226–2230.

AUTHORS

Hasibul Alam received the B.Sc. in Computer Science and Engineering from Daffodil International University, Dhaka, Bangladesh, in 2015 and a M.S. degree in computer science from Jahangirnagar University, Dhaka, Bangladesh, in 2018. Currently, he is pursuing a second master's degree in Computer Science in The University of Texas Rio Grande Valley, Texas, USA. His research interests include IoT, blockchain, and machine learning.

Dr. Emmett Tomai is currently serving as department chair and professor of computer science department at the University of Texas Rio Grande Valley. He received his BS in Computer Engineering and BS in Electrical Engineering degree from Northwestern University, USA in 1997. He completed MS in Computer Science in 2007 and Ph.D. in Computer Science in 2009 from the Northwestern University. He works in the field of artificial intelligence, on language, narrative and video games.