Exploring The Security Issues in Home-Based IoT Devices Through Denial of Service Attacks

Otily Toutsop
Morgan State University
Department of Computer and Electrical Engineering
Baltimore, Maryland - 21251
Email: ottou1@morgan.edu

Sanchari Das
University of Denver
Department of Engineering and Computer Science
Denver, Colorado - 80208
Email: Sanchari.Das@du.edu

Kevin Kornegay
Morgan State University
Department of Computer and Electrical Engineering
Baltimore, Maryland - 21251
Email: kevin.kornegay@morgan.edu

***Abstract*—Internet of Things (IoT) has infiltrated the digital realm, and critical efforts are being made to create robust security for these technologies. However, with increasingly sophisticated attacks, it is essential to understand IoT device security in depth. To understand the device vulnerabilities from the network level, we orchestrated Denial of Service (DoS) attacks for four different IoT devices through network flooding. We conducted our experiment in the lab environment using other IoT devices that include the Amazon Echo, a smart light-bulb, a smart camera, and a smart garage door opener. To conduct the DoS attack, we used Raspberry Pi as the main target to access other network devices with different protocols. We generated the DoS attack using Kali Linux installed in a virtual environment. This experiment demonstrated that hackers might exploit sensor vulnerabilities to gain unauthorized network access and use user data through various IoT devices. We proposed an effective Intrusion Detection technique using a combination of machine learning classifiers and deep learning. Some of the machine learning models include the logistic regression, decision tree, random forest and support vector machine to detect and mitigate the attack. The outcomes show the algorithm which presents the highest degree of attack detection accuracy. Our findings also show that DoS attacks continue to be a significant concern even with improved technologies and security protocols. Finally, we provide design implications to address such critical security flaws.**

***Keywords*—** Denial of Service (DoS) attack, Home Automation, Internet of Things (IoT), TCP SYN Flood, smart devices, smart home, Z-WAVE protocol

I. Introduction

As technology has become more prevalent in our daily lives. People acquire more digitally interconnected devices to help them with their daily activities. As a result, the Internet of Things is one of the most popular technologies used in innovative home systems to date [1]. Figure 1 demonstrates the Internet of Things Security market's rapid growth in various regions, including North America, Europe, Asia Pacific, and ROW (Rest of the World). By 2026, the market is estimated to be worth up to $42 billion.

The Internet of Things (IoT) can be thought of as a network of interconnected devices that communicate through various communication protocols such as WiFi, Bluetooth, Z-wave, and Zigbee [2]. Smart cities, smart transportation, smart healthcare, smart grids, and smart homes are just some applications for IoT devices and technologies. These technologies also allow mobile applications and other monitoring software to track their home appliances via smartphones. For example, a customer with a collection of devices

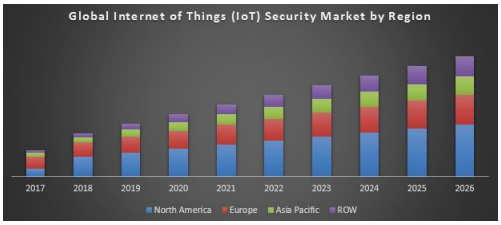

Fig. 1. Global IoT Security Market Revenue Between 2017 and 2026. Source: Global Industry Analysis for Forecast

at home, such as a thermostat, a Ring doorbell, a camera, and light bulbs, can easily monitor them via their smartphone. Unfortunately, IoT devices may have limited technical aspects, such as limited memory capacity, and do not always have sophisticated security features built-in, which can be a significant concern in the cyber-security space [3].

An attacker may use those devices' vulnerabilities to conduct malicious activities on the consumer's network. These flaws include a lack of proper software maintenance protocols, weak passwords, easily accessible computer firmware, inferior privacy security methods, a lack of physical hardening, and a lack of robust encryption algorithms, all of which make data transfer vulnerable [4]. As a result, ensuring the confidentiality and credibility of these devices is crucial and also to ensuring that the system operates correctly and without risk. A network may be subjected to various attacks, including a Man in the Middle (MIM) attack, a Denial of Service (DoS) attack, a downgrade attack, a SQL injection attack, and ping death [5].

Previous research has shown that insecure interfaces in IoT applications may also lead to vulnerabilities, offering attackers the opportunity to infiltrate the consumer's network illegally [6]. A denial-of-service (DoS) attack is a form of cyber-attack in which the attacker attempts to bring down the entire system by sending several network packets. A Denial of Service attack aims to disrupt network services and cause harm, such as stopping network services, cutting connections, and making network resources unavailable, according to [7]. The effects of Denial of Service attacks are enormous, causing significant harm to home users. Furthermore, infiltrators can steal personal user data, kill the target system, and alter the information system. In worst-case cases, a stranger residing abroad will monitor the entire household, according to [4].

To mitigate the issues, we were inspired to investigate IoT vulnerabilities and raise user awareness. As a result, for this study, we primarily used the TCP SYN Flood attack, which makes resources inaccessible to legitimate traffic by flooding the target system with

TCP (Transmission Control Protocol) packages. These resources become unavailable and cannot be accessed by all applications, demonstrating the weakness of a simple DoS attack. The possible implications of these heinous attacks are often understated. The network traffic packets are then examined based on their potential source and destination IP addresses. Questions addressed in this paper include the following.

- What are the different security and protocol vulnerabilities of home-based IoT devices as exposed by Denial of Service attacks?
- How can we design security framework to detect and protect against DoS attacks for home-based IoT devices?

The contribution of this paper is as follows:

1) We explore the smart home network with a different set of devices such as smart light bulbs, a smart camera, a smart garage door, and amazon echo voice assistant.
2) We perform the Denial of Service attack on the based home network and examine the network traffic behavior.
3) We address the critical security vulnerability faced by the smart home network.
4) We propose a new Denial of Service detection technique using a machine learning classifier.
5) We design a secure architecture Data Flow Diagram (DFL) to understand the attack patterns.

The remainder of this paper is structured as follows. Section II presents the risk associated with IoT devices , and in section III, we provide an overview of the latest literature describing IoT vulnerabilities and security threats. Section IV shows how we launched the Denial of Service attack operation, and section V shows the results of the attack. In section VII, we outline our future work direction while noting some limitations of this work, and the conclusion is provided in section VIII.

II. Risk Associated with the Internet of Things Devices

Wongvises et al. investigate a fault tree study for smart home appliances and the invention of intelligent home appliances derived from the Internet of Things [8]. According to the writers, smart home light bulbs offer consumer convenience by automating light control services from anywhere in the house or over the network or Internet. According to the paper, intelligent homes have embedded chips that allow the system to connect to the network. Their research also shows that protection is one of the essential concerns in smart home applications. However, an intelligent home system may offer more vigilance and comfort for a homeowner. It can also jeopardize and inconvenience the homeowner if proper security measures are not in place. To discourage malicious acts from occurring in the first place [9], [10]. In addition, the non-certified system can lack a security feature capable of ensuring the confidentiality, fairness, and availability of the core security principles.

III. Related Work

Kevin Ashton pioneered the Internet of Things idea in 1959, according to [11]. With the explosion of the Internet, IoT has expanded exponentially, and the vital benefits provided by IoT devices have attracted many researchers, businesses,homeowners, and governments [11], [12].Any user can benefit from IoT infrastructure if they have the means to support the connectivity [10]. A simple description of the Internet of Things may be a massive network of interconnected devices with built-in software that collects and shares data from multiple devices across the network. The first cutting-edge example of IoT devices was in 2016 when an article titled "The IoT Architectural Architecture, Design Issues, and Application Domains" demonstrated the architectural framework for IoT devices [13]. It also provided the structural composition of IoT devices with their various components and related issues with some designs and the domain in which those devices are likely to work [14].

The article provided that IoT has been made known as a new wave of Information and Communication Technology (ICT) advancements; It also stated that IoT applications and scenarios are increasing and impacting people's lives every day [15]. In laying out the architectural framework of IoT devices, the article provided that there have been multiple architectural frameworks of IoT devices in numerous areas such as international standard organizations, academia, and research institutions, companies, and civil societies [16].

Besides, with the Internet of Things technologies demands rising, people use smart home devices for their home automation and utility management services. Research conducted by Cope et al. [17] shows that IoT devices have been increasing from time to time. IoT devices include low-power small Internet-enabled devices, smart home refrigerators, smart light bulbs, smart home appliances, home monitoring cameras(surveillance and baby monitoring).Moreover a smart devices are connected to home networks and the Internet. Research conducted in 2018 shows that 23.14 billion IoT devices are connected to the Internet. According to the same study, by the end of 2021, there will be an additional 7.9 billion devices connected to the Internet and home network. The most common IoT devices are amazon echo, Phillips Hue Light, and home automation key [18]. Some of their vulnerabilities include weak passwords, lack of security protection, outdated firmware, and lack of software updates.

Farooq et al. [19] examine the security risks of the Internet of Things in their work. Data confidentiality, data integrity, and data availability are the primary security issues. Another piece of advice [20] offers on this topic is that they talk about the security difficulties and problems involved with each layer and which security measures are suitable. Authors (in this case, scientists) have taken an interest in analyzing the security issues and functionalities of the Internet of Things. They talk about the design and deployment techniques for IoT security measures. One of those tactics is to put things together depending on where they are and create a security system based on human contact and the group's needs, while the other strategy is to make use of the Internet of Things. Finally, there were discussions regarding the Internet of Things security and possible ways to counter efforts. They spoke about the two separate attacks on WSNs and RFID devices, as well as potential countermeasures. Proposed remedies include regulating the transmitted power, which is a means of transmitting a radio signal.

Otmane et al. [21], Ning et al. [22] goes on to speculate on the future of IoT security architecture, arguing that there are three main security areas that all IoT devices need to address: the information, the physical, and the administrative. This paradigm incorporates a social layer, intelligent behavior, and compatibility for security as the fundamental requirements for information security. In a recent paper published in The International Journal of Next-Generation Information Security, Dao et al. [23] address the heterogeneous IoT networks characterized by diverse access technologies and mobile edge computing capabilities and protect them from intelligent DDoS attacks. Instead of stopping distributed denial of service assaults, the proposed solution is a framework called MECshield, which has a centralized controller and many agents distributed around the edges of each local network. This enables the network to fight against malicious traffic.

Researchers [24] delved into the malware in the Internet of Things with DDoS capabilities—Linux malware, such as trojans and viruses. They demonstrated the increase in the overall popularity of the malware (Hydra, Chuck Norris, Tsunami, Aidra, Spike,

Mirai, show).

A. IoT Devices Functionality

The exponential growth of the Internet of Things, wireless technology, and the pervasiveness of smartphones and connected devices, home automation in every home is now a real possibility. A smart home is a network of sensors and controls that work together to provide the user with remote control of various devices. The sensors detect various changes, track them, store the data, and display it for analysis and management. An intelligent home supports ease of use, and it can be handled using a wide range of devices such as a desktop, laptop, tablet, or smartphone [25]. Statista estimates that smart home security is forecast to grow to 22 billion U.S. dollars worldwide in size by 2021.

Smart home System allows homeowners to access and control devices in their homes remotely from anywhere in the world using smartphones and smart devices [26]. In smart home systems, tools such as appliances, cooling systems, lights, smart TVs, and car garages are connected to a controllable network that can be operated remotely. Home security in smart home Systems includes the house locks, smart lights, smart thermostats, surveillance cameras, and smoke detectors [27]. The IoT devices can provide significant benefits, but they also contain vulnerabilities that malicious actors can exploit. One of the most critical issues associated with smart homes is security [6]. Connecting smart home appliances to the Internet increases the risk of malicious attacks. These attacks can compromise a smart home device or system's availability, confidentiality, the integrity of data, and the privacy of the homeowner [16]s. Breaching one of these essential security areas may cause critical security problems in the home system.

One of the main essential characteristics of an IoT device is processing the information or any data quickly [28], [29], [3]. The manufacturers of those devices potentially designed them for a specific purpose enhancing the consumer's life quality. The interactions between those devices facilitate the integration of the sensors in any given network. Four significant components constitute the IoT network [30]. The first components are sensors that sense the real world's physical environment and measure data in an electrical signal [31]. An example of a sensor could be a smoke detector system that senses the smoke in the home. Another example of a sensor could be a smart camera that detects a stranger's presence in any environment[32]. Given that it is a critical component within the smart home, the attacker could exploit that smart camera's vulnerability to spoof the user's network. The second element found within the IoT system is connectivity. The data processing phase allows the device to collect data and send it over to the cloud and, finally, the user interface to receive the information from the sensor. The tools will need to communicate with each other using communication protocols such as WiFi, Zigbee, Bluetooth, and Z-wave [33].

B. IoT Device Security

Abomhara et al. [34] described smart devices as IoT as extensions of the Internet into the physical world for interaction with physical entities from the surroundings. A smart light bulb has low computation power; therefore, it is challenging to establish encrypted communication between controller nodes. Anyone with the right tool can capture and manipulate the communication; therefore, it is highly susceptible for man in the middle attack. Most IoT devices are not secured; when the user purchases them, they do not use Smart devices out of the box. The user needs to update firmware and implement a secure configuration on the IoT devices before connecting it to the network. One way to secure IoT devices is through the use of a defense-in-depth strategy [29].

Most IoT devices are vulnerable and have some common vulnerabilities and weaknesses in the attacking surface's IoT layers. Some have higher vulnerabilities in the devices are insufficient authentication, insecure web interface, vulnerable network service, inadequate security configurations, encryption, weak password, insecure firmware, physical security, and 2-factor authentication [4]. Almost all smart home technologies nowadays use radio frequency to communicate with the central hub, nearby nods, or devices. There are some conspiracy theories that all smart home devices use radio frequency, which may cause cancer when we use them at home—however, this hypothesis is not supported by science.

Knowing that IoT devices operate based on their communication protocols, they can provide multiple advantages for industries and different environments. However, blind spots and security risks can arise in the form of vulnerabilities [35]. The components of IoT devices such as things or devices, the gateway, the cloud, analytics, and user interface are sources to vulnerabilities [36]. Consequently, this can have an impact on millions of devices that consumers use. Finally, the final vulnerability is that users lack security awareness, leading to IoT devices' exposure to vulnerabilities and attacks. These vulnerabilities of IoT devices allow hackers to use them as springboards for their attacks.

C. Protocol Vulnerabilities

Several papers have addressed the vulnerabilities of the Z-Wave protocol. To better conduct research in this area, these works were reviewed to understand the research landscape and to identify the gap. Phan Minh et al. have developed and implemented a Z-Wave gateway controller for a smart home automation system [16]. However, the vulnerabilities associated with the proposed devices were not taken into consideration. In this work, we address those devices' vulnerabilities by launching the Denial of Service attack on the smart home network. Lulu et al. presented a method to launch a Denial of Service attack on a simple Internet of Things (IoT) system using Kali Linux [32]. The authors successfully performed the attack, but with the focus on devices that are IP compatible. However, The approach mentioned in this paper considered both IP and non IP compatible devices giving that a single point of failure or any open port can affect the behavior of the network. To date, prior researchers have successfully designed Z-Wave gate controllers that enable Z-wave devices to interact with other devices on the Internet, but several aspects need to be added to complement previous work in the area, namely:

1) the security aspect of the proposed Z-Wave controller needs to be more examine to address their potential vulnerability. The controller is one of the key elements in the smart home network, and the manufacturer needs to design a gateway with more security controls.
2) The emphasizing on the vulnerability of non-IP compatible devices.
3) the details about the experiment's architecture leading to understanding better the network behavior and some of the security measures that need to be taken for better protection.
4) Analysing some of the protocols used by smart home's devices with their technical definitions will.

IV. Methodology To Launch The DoS Attack

A. Proposed System Model

The architecture depicts a real-world attack scenario. There are many z-wave devices at the lower level, including a thermostat, light bulb, garage door, and door lock. At the higher stage, there are IP-compatible devices that can communicate with the Internet without passing through the raspberry-pi gateway. Non-IP devices are limited devices with a limited processing capacity that is unable to support the encryption algorithm. Z-wave and Zigbee are two protocols used by those restricted devices to communicate. As shown in Figure 2, Zigbee and Z-wave devices represent the point of entry of the network. Those devices use a gateway as a translator

TABLE I
COMPARING PRIOR RELEVANT WORKS ON IOT DEVICES BY EVALUATING THEIR CONTRIBUTION TO THE SCIENTIFIC COMMUNITY

Authors	Title of the paper	Contributions
Ala Al-Fuqaha et al. [11]	Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications	The authors presented some key challenges related to the most relevant IoT protocols
Gordon et al. [12]	Security and Privacy Analyses of Internet of Things Children's Toys	The authors addressed the security issues and privacy related to the usage of small IoT Toys devices
Asghari et al. [10]	Internet of Things applications: A systematic review	This paper gave an overview of different Internet of Things applications and emphasized on their security concerns as well
Gardasevic et al. [13]	The IoT Architectural Framework, Design Issues and Application Domains	The authors of this work presented an architectural framework for designing Internet of Things devices
Minoski et al. [14]	Defining Quality of Experience for the Internet of Things	This paper explored the quality and experienced of some Internet of Things devices without an emphasize on their security aspect
Jose et al. [37]	Smart Home Automation Security: A Literature Review	In this paper, the authors exposed the security issues in smart home automation systems

to send the information out to the cloud. On the other hand, IP compatibles can send the data out directly to the cloud without requiring any translator.

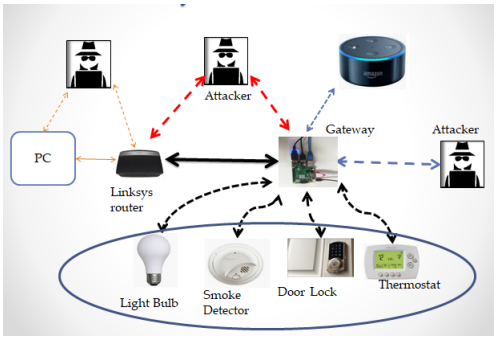

Fig. 2. Design Implementation Of The DoS Attack Which Exploits Critical Security Failures For Internet of Things (IoT) Devices.

B. Denial of Service Attack

A Denial of Service (DoS) attack is a type of cyber-attack launched by overwhelming or flooding the target node with request until regular traffic becomes unavailable. This attack is very critical and could potentially impact the entire system. This form of attack usually results in sluggish behavior, the target system crashes, or the server becomes unavailable [38]. This type of attack often exploits the security vulnerabilities present in the network, software, and hardware design [3]. Several parameters show that a Denial of Service attack is underway, such as the SYN Packages and the SYN-ACK (meaning Acknowledgement).

To connect to an access point (AP), the device needs to associate with the access point before it can begin to exchange data messages. Before the association, the device needs to complete the authentication procedure. If the device wants to disconnect, it sends a disassociation frame to the access point. According to the 802.11 network standards, the de-authentication or disassociation frames are unencrypted and do not require authentication. The lack of encryption can be exploited; an attacker can easily spoof the MAC address of the device or the access point to make a de-authentication request on behalf of the target. The attacker can craft these frames and send them to the access point so that the access point assumes the frames to be coming from the device and not the attacker.

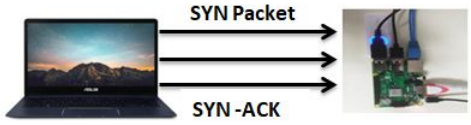

Fig. 3. A Snapshot of the Syn-Flooding Attack Between the Attacker's Device and The Vulnerable IoT Devices.

The SYN-flooding attack is typically based on the Transmission Control Protocol (TCP) three-way handshake. The entire process is to flood as many TCP ports on the target system with SYN messages to start the communication between the attack machine and the target system [39].

C. Hping3

Hping3 is a more advanced and widely used tool by an ethical hacker to damage the targeted system. This tool uses TCP, UDP, ICMP, and RAW-IP protocol and can circumvent the firewall filter. Furthermore, Hping3 is responsible for handling fragmentation; packets' body could be used to transfer encapsulated files. Using Hping3, many tasks can be performed, such as firewall tests, advanced port scanning, remote OS fingerprinting, TCP/IP stack auditing, and test network conducting using different protocols.

ICMP is the Internet Control Message Protocol layer used by network devices to detect network communication issues. This protocol is also used to find out whether or not data is reaching its

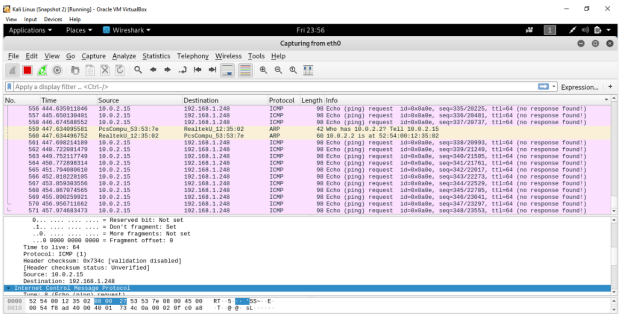

Fig. 4. Simple Internet Control Message Protocol (ICMP) Communication Pings Between Amazon Echo Device and The Exploited Light Bulb Using Wireshark

destination. Moreover, the ICMP protocol provides some information about the device's status when something goes wrong in the network.

V. Experimental Results and Analysis

The attack was launched in the lab, where we have a network setup that includes a smart door lock, a smart thermostat, a smart Amazon Echo, a smart fridge, a smart smoke detector, and a smart light bulb. Here is the output of the experiment:

A. Methodology of the attack scenario

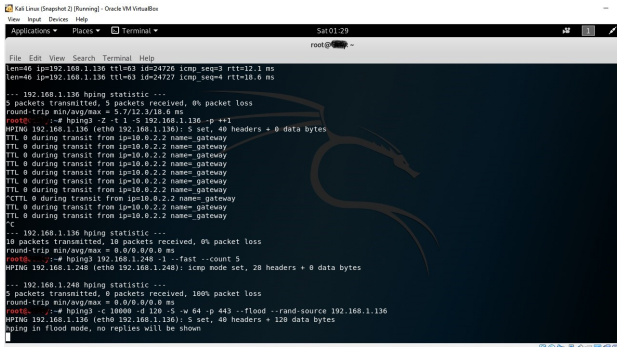

Fig. 5. Screenshot of the Denial of Service (DoS) Attack Set-up in the Home-based Internet of Things (IoT) Network Using Kali Linux Tool, Which is Utilized for Penetration Testing.

Outcomes: The outputs in Figure 4 resulted after the use of the following command Hping3 –c 10000 –d 120 –S –w 64 –p 443 –flood –rand-source 192.168.1.136 to launch the attack on the gateway. "Hping3" is the program command that contents all the packages. "-c 10000" represents the number of IP packets sent to the gateway to use all the resources. "-d 120" means that the size of the packet sent to flood the gateway is 120. This size could be more than 120. "-SYN" signifies that in this experiment, only SYN packets are sent to the gateway. "-w 64" represents the TCP windows size. "-p 443" means that the destination port is 443. "flood" means that packets are sent rapidly.

From Figure 6, we realize that the hacker, from a random IP address, keeps sending SYN flood packages to the victim, the Alexa IP address (192.168.1.248). The packets were created from the different spoofed IP address. Therefore, the Denial of Service (DoS) is successful. This paper also allowed learning of the usage of Kali Linux for ethical hacking. Ethical hacking, also known as penetration testing, involves the same tools, tricks, and techniques hackers use. Ethical hacking is done with the target's authorization. Ethical hacking intends to find out vulnerabilities from a hacker's viewpoint to implement security measures to patch the issue.

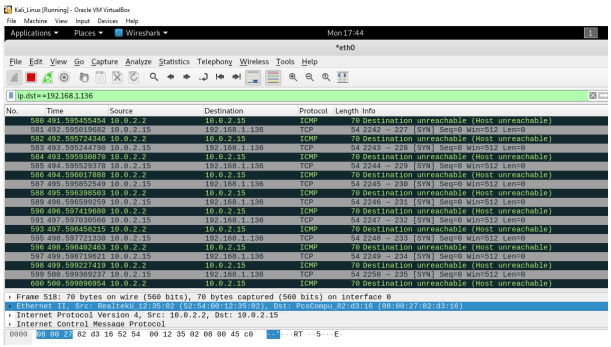

Fig. 6. Screenshot of the Packet Capture (PCAP) Files Showing the SYN-Flooding Attack Traffic on Transmission Control Layer Protocol (TCP-IP).

B. Data Traffic Collection

To get a realistic collection of benign and malicious IoT device traffic, we set up an experimental consumer IoT device network and configure a Raspberry Pi model 3 as a WiFi access point. Then, to make it more user-friendly, we could connect additional IoT devices to the Raspberry Pi's WiFi network. Normal (non-DoS) traffic could be collected by sending packets to all Internet of Things (IoT) devices for 30 minutes and then saving the pcap files. We perform many interactions during daily use, including streaming video to the server, turning devices on and off, and installing firmware updates. Next, we only retain IoT traffic. It is challenging to acquire Denial of Service (DoS) attack data traffic. Our experiment is based on real-time data. The laptop serves as the DoS generator, while the Raspberry Pi could serve as the DoS victim. By connecting both devices over WiFi to our Raspberry Pi 3 access point, we link the two devices together. Each DoS attack class has a definite time separation, and then the DoS attack source can use the victim's IP address for a DoS attack.

C. The Machine Learning Algorithm With The Classifiers

The packet structure captured using Wireshark is the incoming packet structure with 1582681 observations. We use Packet, Time, Source, Destination, Protocol, and Size in our training process. The two classifiers have identical feature sets and are thus put to the test to see which gives the best accuracy. Using Machine learning libraries, Sci-Kit Learn, and Python, we utilize the previously obtained data to train the algorithm. We divide the data into two sets, one set for training and the other for testing. We assign 80% of the data to the 'true' category and 20% to the 'false' category in the training set. Then, we analyze the results using a confusion matrix to check for accuracy. When interpreting the confusion matrix's first diagonal, we know if the results are accurate or not. This next step requires that we have all of the training data as a CSV file in a normalized and scaled form. In order to accomplish this, we will first need to clean the required data, which we can do by creating labels and converting text to relevant numbers [40]. Next, the data is scaled so that it matches the activation function of the ML algorithm. For all these, we used pandas libraries for pythons. Now that we have categorized our data, we can now train our model using two Machine Learning classifiers.Our process is defined as follows: The classification report uses metrics such as accuracy, recall, and f1 score per class to represent the main classification metrics. In addition, true and false positives, true and false negatives, are used to calculate the metrics. Thus, there are four possible outcomes: true, false, or if our predictions were correct or not.

	src_port	dst_port	protocol	flow_duration	flow_byts_s	flow_pkts_s	fwd_pkts_s	bwd_pkts_s	tot_fwd_pkts	tot_bwd_pkts	...
0	9020	44144	6	43753585.0	4.775412e+04	73.685391	43.585000	30.100391	1907	1317	...
1	9673	42417	6	1602.0	8.239700e+04	1248.439451	624.219725	624.219725	1	1	...
2	5353	5353	17	30603.0	7.548280e+03	98.029605	98.029605	0.000000	3	0	...
3	80	54685	6	87161.0	1.079267e+06	780.165441	780.165441	0.000000	68	0	...
4	40811	8820	6	30090452.0	1.648363e+01	0.299098	0.132933	0.166166	4	5	...
...	...	...	...	...	...	...	...	...	...	...	...
17799	8854	554	6	1418.0	7.898449e+04	1410.437236	705.218618	705.218618	1	1	...
17800	3868	554	6	4371.0	2.562343e+04	457.561199	228.780599	228.780599	1	1	...
17801	4458	554	6	3539.0	3.164736e+04	565.131393	282.565697	282.565697	1	1	...
17802	8409	554	6	3543.0	3.161163e+04	564.493367	282.246684	282.246684	1	1	...
17803	80	54695	6	101339.0	1.137825e+06	809.165277	809.165277	0.000000	82	0	...

Fig. 7. Screenshot of the Packet Capture (PCAP) Showing Denial of Service (DoS) Attack data on the Internet of Things devices.

1) True Negative (TN): is a case in which the actual label was negative and predicted negative
2) True Positive (TP): a case in which the actual label was positive and predicted positive
3) False Negative (FN): Represents a case in which the actual label was positive but predicted to be negative.
4) False Positive (FP): Represents a case in which the actual label was negative but predicted positive

The precision represents how accurate the predictions are in the model. It is defined as the ratio of true positives to the sum of true and false positives for each class.

$$Precision = \frac{TP}{TP + FP} \tag{1}$$

The recall represents the percentage of positive cases detected in the model. It is defined as the ratio of true positives to the sum of true positives and false negatives.

$$Recall = \frac{TP}{(TP + FN} \tag{2}$$

The accuracy is the number of correct predictions, which includes both positive and negative predictions, divided by the total number of predictions made.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

Score F1 represents the percentage of correct positive predictions. Score F1 is a weighted harmonic average of precision and recall such that the best score is 1.0, and the worst is 0.0.

$$ScoreF1 = \frac{2(Recall \times Precision)}{Recall + Precision} \tag{4}$$

1) Logistic Regression: For each measure, we take the number of times the corresponding category matches and apply the metric value to the confusion matrix, calculating the following: True Positive, True Negative, False Positive, and False Negative.The output of the confusion matrix is shown in Figure 8.

2) Decision Tree: For each measure, we take the number of times the corresponding category matches and apply the metric value to the confusion matrix, calculating the following: True Positive, True Negative, False Positive, and False Negative. The confusion matrix for the Decision Tree is shown in Figure 9

3) Random Forest: For each measure, we take the number of times the corresponding category matches and apply the metric value to the confusion matrix, calculating the following: True Positive, True Negative, False Positive, and False Negative. The confusion matrix for the Random Forest is shown in Figure 10

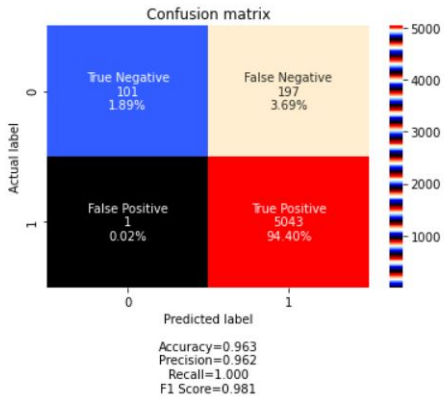

Fig. 8. Confusion Matrix for the Logistic Regression showing the True Positive, the True Negative, the False Negative and the False Positive metrics

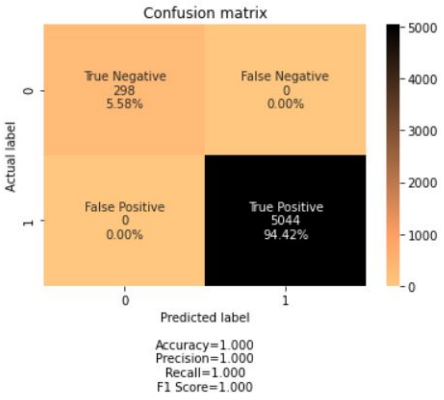

Fig. 9. Confusion Matrix for the Decision Tree showing the True Positive, the True Negative, the False Negative and the False Positive metrics

D. Support Vector Machine

We built our support vector machine model by extracting essential features from the dataset. The output of the SVM is shown in Figure 11.

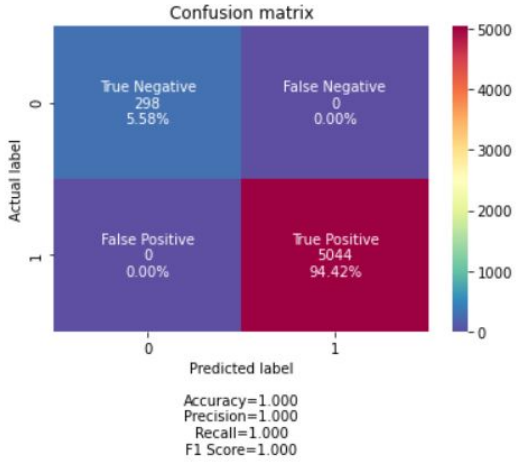

Fig. 10. Confusion Matrix for the Random Forest showing the True Positive, the True Negative, the False Negative and the False Positive metrics

```
Accuracy: 0.9250210614995787
```

Fig. 11. The Accuracy for the Support Vector Machine Model

E. Deep Learning Model

Neural networks are used to create deep learning models. A neural network processes inputs in hidden layers using weights that are adjusted during training. The model then makes a prediction. The weights are adjusted to find patterns and make better predictions. The advantage of this model is that the neural network picks up features on its own, as shown in Figure. The number of epochs represents the number of times our model iterates over the dataset. Eventually, as the number of epochs increases, the model gets better, but only up to a certain point. When that point is reached, the model will no longer be able to get better over time. Also, the longer the model takes to run, the more epochs are required.

```
17804/17804 [==============================] - 7s 397us/step - loss: 4529848.5000 - accuracy: 0.9325
Epoch 2/15
17804/17804 [==============================] - 7s 387us/step - loss: 10524.4053 - accuracy: 0.9389
Epoch 3/15
17804/17804 [==============================] - 7s 390us/step - loss: 1559.6122 - accuracy: 0.9489
Epoch 4/15
17804/17804 [==============================] - 7s 390us/step - loss: 2150.1558 - accuracy: 0.9487
Epoch 5/15
17804/17804 [==============================] - 7s 400us/step - loss: 2250.6458 - accuracy: 0.9487
Epoch 6/15
17804/17804 [==============================] - 7s 403us/step - loss: 402.9636 - accuracy: 0.9486
Epoch 7/15
17804/17804 [==============================] - 7s 398us/step - loss: 0.2027 - accuracy: 0.9486
Epoch 8/15
17804/17804 [==============================] - 7s 387us/step - loss: 0.2028 - accuracy: 0.9486
Epoch 9/15
17804/17804 [==============================] - 7s 384us/step - loss: 0.2027 - accuracy: 0.9486
Epoch 10/15
17804/17804 [==============================] - 7s 389us/step - loss: 0.2027 - accuracy: 0.9486
Epoch 11/15
17804/17804 [==============================] - 7s 396us/step - loss: 2.2304 - accuracy: 0.9486
Epoch 12/15
17804/17804 [==============================] - 7s 391us/step - loss: 0.2027 - accuracy: 0.9486
Epoch 13/15
17804/17804 [==============================] - 7s 389us/step - loss: 0.2028 - accuracy: 0.9486
Epoch 14/15
17804/17804 [==============================] - 7s 398us/step - loss: 0.2029 - accuracy: 0.9486
Epoch 15/15
17804/17804 [==============================] - 7s 388us/step - loss: 0.2028 - accuracy: 0.9486
```

Fig. 12. The deep learning model showing the accuracy and the number of epochs

F. Comparison with other Work

In this work, we examine in detail the behavior of denial of service attacks to readily detect its presence in any given system. Compared with current work on detecting an anomaly with machine learning in the IoT network incursion, our approach also improves the metrics parameters and utilize the deep learning technique as well 14.

G. Mitigation

It is essential to ensure that all penetration testing activities are authorized and within legal limits. Contracting the company and disclosing the vulnerabilities is crucial. The company can patch the vulnerabilities. It is also vital to add countermeasures against the vulnerabilities discovered.As proposed in this research, the machine learning classifiers can be deployed in the home-based IoT system to monitor incoming malicious data traffic limiting the attack damage.

VI. Proposed Security Architecture While Implementing Threat Modeling

Threat modeling is the application security activity to analyze security in software development and provides the system's security view. Phase 1: Perform the denial-of-service attack on the target device to understand its behavior during the process. Phase 2: Using Wireshark to capture the network traffic when the denial-of-service attack happens in the network. Phase 3: Evaluate the communication protocol giving that in the scenario described in this paper, the Raspberry was used as a target to monitor and control the IoT devices.

Some of the communications channels are:

1) Raspberry Pi gateway and smart home devices communicate over Zigbee and Bluetooth.
2) The Amazon echo App and the raspberry pi communicate via WiFi and Bluetooth.
3) The Amazon App and Web endpoint interact over REST API
4) The smart home devices

Nearly all software systems are now facing many risks, and as technology changes, there are more and more threats. Threats can originate from outside or within organizations, and severe consequences might occur. Attacks can stop systems completely, or cause sensitive data to be leaked, which reduces consumer confidence in the system provider. Administrators can utilize "threat-modeling methodologies" to educate defense measures to prevent threats from taking advantage of system failures. Tactics for threat modeling:

- an abstraction of the system
- profiles of prospective assailants including their targets and methods
- a collection of prospective hazards

Many methods have been developed for threat modeling. They can be integrated to create a more robust and more comprehensive perspective of potential dangers. However, they are not all complete; some are abstract and others-centered. Some strategies primarily focus on risks or concerns about privacy. No threat modeling is advised differently; the choices of approaches are based on the demands and specific concerns of the problem. In this work, we proposed an efficient Threat modeling and Security Design Architecture to help mitigate some vulnerabilities of a home-based IoT system. Our proposed secure architecture examines the target components and attack patterns. To perform the security analysis of an embedded system, the proposed approach breaks the system down into different parts and creates a Data Flow Diagram (DFL). One benefit of creating a (DFL) is that it allows developers to understand better the attack patterns and each component's interaction in the system. Another advantage of making the Data Flow Diagram (DFL) is analyzing and figuring out the central point of failures in the system that might cause malicious activities. Lastly, it will also facilitate the evaluation process of finding the likelihood of future exploitation.

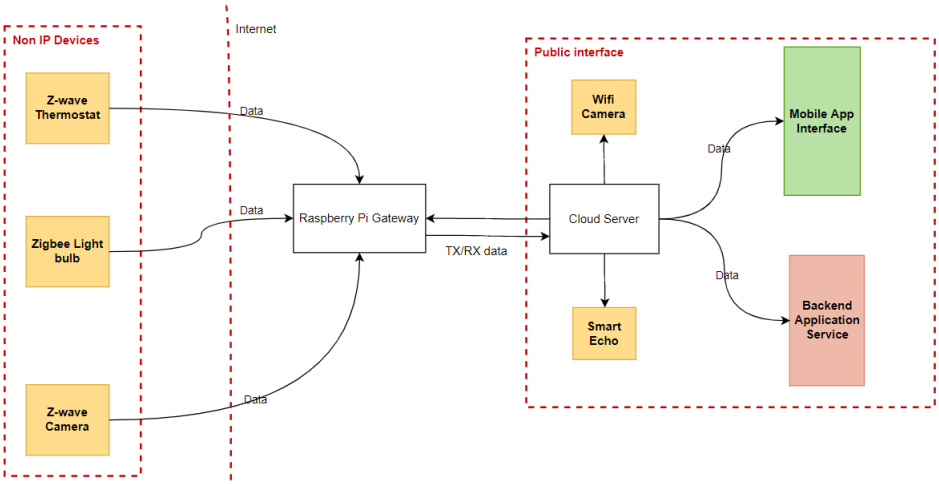

Fig. 13. Proposed IoT Security Design Architecture to Successfully Identify and Mitigate the Denial of Service Attack (DoS) in the Home-based Network.

Fig. 14. A comparison Table between our Approach and Previous Work

Models	Precision	Recall	F1 score	Accuracy
The Approach Implemented in this Paper				
Logistic Regression	0.96	1.00	0.981	0.963
Decision Tree	1.00	1.00	1.00	1.00
Random Forest	1.00	1.00	1.00	1.00
Support Vector Machine	0.93	1.00	0.96	0.925
Deep Learning				0.9486
Ramesh et al.				
	Precision	Recall	F1 Sc	
Decision Tree	0.92	0.92	0.92	
Support Vector Machine	0.89	0.84	0.87	
Random Forest	0.98	0.73	0.93	
Gradient Boosting	0.97	0.73	0.84	

VII. Future Work

This work demonstrated only a specific case of Denial of Service (DoS) attack on the home network and proposed the threat modeling and security architecture of the attack scenario. The global issue face by IoT in today's market is the lack of firmware updates giving that the devices are old and can be used as back doors to attack the entire system. Manufacturers are putting new devices in the market without considering the legacy devices paired to the user's network. Another issue related to this problem is the privacy of the consumers. We would implement several other attacks on a range of smart home devices and networks for our future work and then propose countermeasures to suppress these attacks optimally.

VIII. Conclusion

The overarching aim of the paper was to investigate the security concerns and problems associated with intelligent home-based Internet of Things devices. Building a gateway may aid in avoiding network disclosures if the company goes out of business or closes down. IoT systems have many advantages, but they also have flaws that malicious actors can exploit. Security is one of the most pressing concerns about smart homes. By connecting smart home appliances to the Internet, the chance of malicious attacks increases. These attacks may jeopardize the availability, confidentiality, and integrity of data, as well as the privacy of homeowners, of a smart home device or system. Breaching one of these critical security areas can result in serious security issues with the home system. Furthermore, the commercial hub does not provide enough versatility to the customer. As a result, the entire Z-Wave network was built on the raspberry-pi gateway. The majority of our testbed's equipment was also added to the network. The DoS attack was carried out by flooding the Raspberry Pi gateway with many packets. Wireshark was used to capture network traffic during the attack. We use a combination of machine learning models such as logistic regression, decision tree, random forest and support vector machine as well as deep learning model to evaluate the performance of the proposed Intrusion detection system.

IX. Acknowledgement

We would like to thank the Center for Reverse Engineering and Assurance Laboratory at the Morgan State University and the Security and Privacy Research Lab at the University of Denver.

Any opinions, findings, and conclusions or recommendations expressed in this material are solely those of the authors and do not necessarily reflect the views of the Morgan State University or the University of Denver.

REFERENCES

[1] 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)*, 2020, pp. 272–276.

[2] M. B. Yassein, W. Mardini, and A. Khalil, "Smart homes automation using z-wave protocol," in *2016 International Conference on Engineering & MIS (ICEMIS)*. IEEE, 2016, pp. 1–6.

[3] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, "The z-wave routing protocol and its security implications," *Computers & Security*, vol. 68, pp. 112–129, 2017.

[4] B. Nour, K. Sharif, F. Li, and Y. Wang, "Security and privacy challenges in information-centric wireless internet of things networks," *IEEE Security & Privacy*, vol. 18, pp. 35–45, 2020.

[5] K. Mallikarjunan, K. Muthupriya, and S. M. Shalinie, "A survey of distributed denial of service attack," *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1–6, 2016.

[6] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 636–654, 2016.

[7] R. Paudel, T. Muncy, and W. Eberle, "Detecting dos attack in smart home iot devices using a graph-based approach," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 5249–5258.

[8] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, "Fault tree analysis-based risk quantification of smart homes," *2017 2nd International Conference on Information Technology (INCIT)*, pp. 1–6, 2017.

[9] R. A. Hallman, J. Bryan, G. Palavicini, J. DiVita, and J. Romero-Mariona, "Ioddos - the internet of distributed denial of sevice attacks - a case study of the mirai malware and iot-based botnets," in *IoTBDS*, 2017.

[10] P. Asghari, A. Rahmani, and H. Javadi, "Internet of things applications: A systematic review," *Comput. Networks*, vol. 148, pp. 241–261, 2019.

[11] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, pp. 2347–2376, 2015.

[12] G. Chu, N. Apthorpe, and N. Feamster, "Security and privacy analyses of internet of things children's toys," *IEEE Internet of Things Journal*, vol. 6, pp. 978–985, 2019.

[13] G. Gardasevic, M. Veletic, N. Maletic, D. Vasiljevic, I. Radusinovic, S. Tomovic, and M. Radonjic, "The iot architectural framework, design issues and application domains," *Wireless Personal Communications*, vol. 92, pp. 127–148, 2017.

[14] D. Minovski, C. Åhlund, K. Mitra, and R. Zhohov, "Defining quality of experience for the internet of things," *IT Professional*, vol. 22, pp. 62–70, 2020.

[15] M. Z. Chaari and S. Al-Máadeed, "Wireless power transmission for the internet of things (iot)," *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, pp. 549–554, 2020.

[16] H. Jiang, C. Cai, X. Ma, Y. Yang, and J. Liu, "Smart home based on wifi sensing: A survey," *IEEE Access*, vol. 6, pp. 13 317–13 325, 2018.

[17] P. Cope, J. Campbell, and T. Hayajneh, "An investigation of bluetooth security vulnerabilities," in *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2017, pp. 1–7.

[18] J. A. Ahmed, *Web penetration testing with Kali Linux*. Packt Publishing Ltd, 2015.

[19] M. Farooq, M. Waseem, A. Khairi, and P. Mazhar, "A critical analysis on the security concerns of internet of things (iot)," *International Journal of Computer Applications*, vol. 111, pp. 1–6, 02 2015.

[20] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[21] O. E. Mouaatamid, M. Lahmer, and M. Belkasmi, "Internet of things security: Layered classification of attacks and possible countermeasures," *Electronic Journal of Information Technology*, 2016.

[22] H. Ning and H. Liu, "Cyber-physical-social based security architecture for future internet of things," *Advances in Internet of Things*, vol. 02, 01 2012.

[23] N.-N. Dao, T. V. Phan, J. Kim, T. Bauschert, S. Cho *et al.*, "Securing heterogeneous iot with intelligent ddos attack behavior learning," *arXiv preprint arXiv:1711.06041*, 2017.

[24] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "Analysis of ddos-capable iot malwares," in *2017 Federated Conference on Computer Science and Information Systems (FedCSIS)*. IEEE, 2017, pp. 807–816.

[25] M. Taylor, D. Reilly, and C. Wren, "Internet of things support for marketing activities," *Journal of Strategic Marketing*, vol. 28, pp. 149 – 160, 2020.

[26] S. Munirathinam, "Chapter six - industry 4.0: Industrial internet of things (iiot)," *Adv. Comput.*, vol. 117, pp. 129–164, 2020.

[27] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home iot privacy," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, pp. 1 – 20, 2018.

[28] Z. Ning, P. Dong, X. Kong, and F. Xia, "A cooperative partial computation offloading scheme for mobile edge computing enabled internet of things," *IEEE Internet of Things Journal*, vol. 6, pp. 4804–4814, 2019.

[29] T. Alam, "Internet of things: A secure cloud-based manet mobility model," *Int. J. Netw. Secur.*, vol. 22, pp. 514–520, 2020.

[30] P. I. Radoglou-Grammatikis, P. Sarigiannidis, and I. Moscholios, "Securing the internet of things: Challenges, threats and solutions," *Internet Things*, vol. 5, pp. 41–70, 2019.

[31] R. K. Chahal, N. Kumar, and S. Batra, "Trust management in social internet of things: A taxonomy, open issues, and challenges," *Comput. Commun.*, vol. 150, pp. 13–46, 2020.

[32] Y. Lu and L. D. Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," *IEEE Internet of Things Journal*, vol. 6, pp. 2103–2115, 2019.

[33] E. Lara, L. Aguilar, M. A. Sanchez, and J. A. Garcia, "Lightweight authentication protocol for m2m communications of resource-constrained devices in industrial internet of things," *Sensors (Basel, Switzerland)*, vol. 20, 2020.

[34] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobil.*, vol. 4, pp. 65–88, 2015.

[35] J. Shin, Y. Park, and D. Lee, "Who will be smart home users? an analysis of adoption and diffusion of smart homes," *Technological Forecasting and Social Change*, vol. 134, pp. 246–253, 2018.

[36] A. Iqbal, F. Ullah, H. Anwar, K. Kwak, M. Imran, W. Jamal, and A. ur Rahman, "Interoperable internet-of-things platform for smart home system using web-of-objects and cloud," *Sustainable Cities and Society*, vol. 38, pp. 636–646, 2018.

[37] A. C. Jose and R. Malekian, "Smart home automation security: A literature review," *Smart Comput. Rev.*, vol. 5, pp. 269–285, 2015.

[38] S. Alanazi, J. Al-Muhtadi, A. Derhab, K. Saleem, A. N. AlRomi, H. S. Alholaibah, and J. J. Rodrigues, "On resilience of wireless mesh routing protocol against dos attacks in iot-based ambient assisted living applications," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom)*. IEEE, 2015, pp. 205–210.

[39] S. S. I. Samuel, "A review of connectivity challenges in iot-smart home," in *2016 3rd MEC International conference on big data and smart city (ICBDSC)*. IEEE, 2016, pp. 1–4.

[40] O. Toutsop, P. Harvey, and K. Kornegay, "Monitoring and detection time optimization of man in the middle attacks using machine learning," in *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, 2020, pp. 1–7.