Deploying Man-In-the-Middle attack on IoT devices connected to Long Range Wide Area Networks (LoRaWAN)

Deploying Man-In-the-Middle Attack on IoT Devices Connected to Long Range Wide Area Networks (LoRaWAN)

Alessandra Alvarez Olazabal[1]
School of Computing and Eng
University of West London
United Kingdom
21466822@student.uwl.ac.uk

Jasmeet Kaur[2]
School of Computing and Eng
University of West London
United Kingdom
21503866@student.uwl.ac.uk

Abel Yeboah-Ofori[1]
School of Computing and Eng
University of West London
United Kingdom
abel.yeboah-ofori@uwl.ac.uk

***Abstract*: Advancements in research and innovation on Smart IoT technology have provided quality of life to physical and visually impaired users. However, deploying Man-In-the-Middle (MITM) attacks on IoT devices that use Long Range Wide Area Networks (LoRaWAN) has increased exponentially due to the high user demand and increased access to the internet. As a result, there is a high probability of user data being exploited, especially on visually impaired user IoT devices, by penetrating the network devices leading to cyberattacks such as remote access, extortion, sabotage, and loss of internet access. This paper explores the methods used by threat actors to deploy MITM attacks on IoT devices that use LoRaWAN to detect vulnerabilities, understand attack patterns and assist in understanding human factors in cyber security. The contribution of this paper is threefold: First, we review the existing attacks on IoT devices and their impact on visually impaired users. Secondly, we implement a MITM attack using an open-source tool to exploit the LoRaWAN to determine the vulnerabilities. Finally, we recommend a control mechanism to improve security. The results show that the MITM attack can be replicated on devices, demonstrating the importance of creating more robust security to prevent information or identity theft without the user's permission.**

***Keywords**: Cyberattack, LoRaWAN, Man-In-The-Middle Attack, Internet of things, Cybersecurity, ARP Spoofing.*

I. INTRODUCTION

The Internet of Things (IoT) connects smart devices with each other to enable the exchange of information, services, and goods over the same network [1]. These IoT devices are equipped with enhanced intelligence and sensors, which makes it easier to share information with users at any time [2] including smart homes, health monitoring, control, and location of pets. Furthermore, IoT devices are built with sensors and actuators that can process signals and generate data constantly [3] in a complex construction of diverse types of technological layers that work together to make users' lives easier [4]. The IoT has evolved through the years from the initial use of RFID connectivity to electronic product codes [3[[4] to connect physical devices to communicate with each other using sensors and actuators, including nanotechnology miniaturization technologies and the internet. The essence of the IoT innovations is to provide connectivity and improve the quality of life for users, the economy and industries, including healthcare, education, energy, water, manufacturing, transport and communication and [5] [6] [7]. Unfortunately, these connectivities have been susceptible to MITM attacks on the IoT architecture, leading to compromises on the integrated perception, network and application layers and the connected devices [1]. The most affected are the visually impaired users [6] since they rely heavily on these embedded processes in smart devices such as smartphones, T.V.s, and Cameras to interact with remote services using the internet, cloud and data centres for their daily activities. Sobnath et al. posit that about 110 million visually impaired people are experiencing challenges in using IoT devices. Thus, adaptive research and innovative solutions are required seamless interaction between the visually impaired person and devices [6].

The LoRaWAN connectivity is used on IoT devices in an intelligent network environment. Its network structure and operations have different characteristics and specific typologies that are considered the "Star-of-stars" topology. Different connection elements are combined and implemented in multiple devices to create smart cities, as depicted in Figure 1.

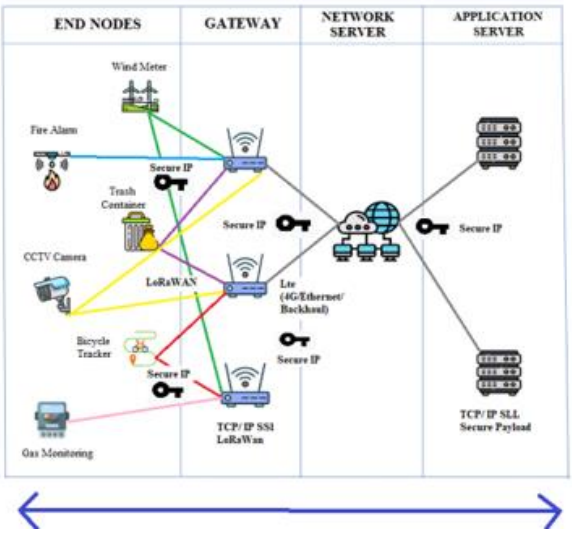

Fig 1. LoRaWAN Network Structure

Figure 1 discusses the LoRaWAN structure that is divided into four different sectors, including the nodes, gateways, network and application servers as follows:

- End devices (nodes): Consist of connecting physical devices, including sensors or switches, to the network through gateways using LoRa RF modulation [8] [9].
- Gateways: Establish send or receive communication from the device to the internet registered to a specific server in different channels, ranging from 3G to 5G.
- Network Server: Manages devices connected in the network, establishing connections and at the same time confirming the authenticity and integrity of messages [8].
- Application Server: Considers how the data is processed, transmitted and analyzed from one device to another across the network, using different techniques.
- Join Server: Manages the flow of the LoRaWAN, where the delivery of the message sent through a request to join the server using NwKSkey, and AppSkey could occur directly or vice versa. [8] [9].

Deploying MITM attacks on IoT devices that use Long Range Wide Area Networks (LoRaWAN) have increased exponentially due to the high user demand and increased access to the internet. As a result, the probability of user data being exploited by third parties by penetrating the network devices using remote access tools leading to cyberattacks such as false data injections, extortion, sabotage, and internet access loss, has increased. Thus, understanding human factors in using IoT devices can improve cyber security controls. LoRaWAN is a low-power, wide-area wireless communications technology that connects IoT devices with LoRaWAN gateways, I.P. networks, servers, and network applications. Figure 1 depicts a conceptual model of the LoRaWAN architecture.

This paper explores the methods used by threat actors to deploy MITM attacks on IoT devices that use LoRaWAN to detect vulnerabilities, understand attack patterns and provide security recommendations. The contribution of this paper is threefold: First, we explore existing attacks on IoT devices and their impact on the user and human factors. Secondly, we implement MAIM attacks using an open source tool to exploit the LoRaWAN to determine the vulnerabilities. Finally, we recommend a control mechanism to improve security.

II. RELATED WORKS

This section reviews related works and the start-of-the-art of Smart City architectures and IoT device vulnerabilities and cyberattacks on LoRaWAN and its impact on visually impaired users. The study considers the IoT security architectures and how the related implementations impact devices. These include identifying previous classification approaches that leverage the LoRaWAN structures, including the nodes, gateways, network servers and application servers and how they are integrated.

Regarding the different attacks that can affect IoT devices, [1] posits that attackers can exploit vulnerable devices or cloud-based applications and steal data or users' identities on unprotected devices. The authors explored IoT attacks and challenges by evaluating the IoT architecture, the three perception, network and application layers and how MITM attacks can be deployed on the architecture [1]. The authors emphasized technological and security challenges in the layers, including wireless and RFID and how the sensors lead to exposures. Further, Abdulrahman and Varol explored the issues of defending against cyber-attacks on IoT devices, issues of understanding attack motives, and the challenges of implementing security mechanisms to prevent attacks on IoT devices [10]. The authors postulate that one of the ways to prevent the attacks is to understand how vulnerable spots on IoT devices are exploited to trace back to the weakest link of the network [10]. Regarding intelligent mechanisms that can detect unfamiliar intrusions and find unusual activities, Tabassum & Lebda, consider the Helium hotspot and its complexities in smart IoT, giving the possibility to attackers to turn devices such as T.V., watches, CCTV cameras, and even smart pet collars into harmful botnets to be attacked [11]. Biswajit reviewed LoRaWAN architecture by exploring the various network features and the different LoRa from wireless technologies in long-range transmissions with low power consumption [8]. Ingham et al. analyzed IoT security vulnerabilities on devices and their predictive signal jamming attacks on LPWAN and LoRaWAN by designing and simulating predictive models on device data generations. The authors highlighted security issues, including connecting inferior devices, using less mature standards, and sending small amounts of data on enabled devices over a long distance, leading to IoT vulnerabilities. [12]. There are various categories where an IoT device can be classified: Wearable devices, smart home devices, and M2M. A cyber-attack is launched from one to different on IoT devices. The complexity of smart IoT allows attackers to turn devices such as T.V.s, watches, CCTV cameras, and even smart pet collars into harmful botnets to be attacked. Thus, the diverse types of threats and vulnerabilities in IoT and networking affect various levels of cybersecurity [13]. Lee surveyed IoT architecture that enables five-layer corporate IoT architecture and focuses on cybersecurity challenges and solutions at the layer level [14]. The perception layer where devices capture a large quantity of real-time data needs different energy-saving strategies. Lopez et al. posit that the cloning of device chips by attackers is a crucial security concern at the perception layer as DDoS attacks might be launched using clones of RFID tags [15]. Further, Sobnath et al. reviewed smart cities comprehensively to improve mobility and quality of life for visually impaired IoT device users. The authors consider challenges such as issues of mobility and navigation through known and unknown obstacles that, when addressed, could provide more independence and safety [6]. Furthermore, Martini et al. explored the intrinsic characteristics required to implement quality of experience (QoE) as opposed to the quality of services (QoS) to evaluate the user-centric design for novel multimedia systems and standards. The authors postulate that focusing on QoS relies on network performance without emphasis on perceived quality [16]. Moreover, Nasralla proposed a novel methodology to design sustainable virtual reality patient rehabilitation systems with IoT sensors using virtual smart cities using time series analysis to identify malfunctioning IoT devices [7]. Additionally, Rehman et al. investigated the m-QoS analysis of medical video streaming using a small cell installed inside an ambulance by considering a heterogeneous network including a macrocell with a centric eNodeB coexisting with a mobile cell [17]. Subsequently, Rehman et al. analyzed mobile app features for people with Autism in a post Covid-19 Scenario by identifying several highly rated mobile applications designed to assist people with Autism Spectrum Disorder (ASD) using the PRISMA methodology. The authors identify challenges such as verbal and non-verbal communication, social understanding and behaviour, inflexible behaviour and a lack of imagination as critical issues facing ASD people as rationale [18]. Khattak et el. proposed a single anchor localization approach for wireless sensors in a 5G satellite-terrestrial network by using an algorithm with bidirectional information mobility focused on short paths with two beacon points [19]. Naoui et al. explored how third-party-based key management could enhance the LoRaWAN security architectures and the enabled IoT devices using the scythe tool to evaluate security [20]. Dofe et al. reviewed hardware trojan and side-channel analysis attacks on emerging IoT applications by proposing a low-cost dynamic permutation method for IoT device attacks [27].

All the related works are relevant to IoT security and could assist visually impaired users. However, we proposed a conceptual model and deployed a MITM attack on LoRaWAN devices using the Kali Linux tool

to deploy the attack and used Wireshark to analyze I.P. address vulnerabilities to provide security controls.

III. APPROACH

This section considers the different approaches to initiating attacks on IoT devices to determine the vulnerable spots and the challenges in securing the devices. First, we implement MITM attacks using Kali Linux, an open-source tool to exploit the LoRaWAN to determine the vulnerabilities. Then, figure 2 incorporates security into the IoT architecture.

A. *LoRaWAN Security Architecture*

The proposed LoRaWAN security architecture consists of four components integrated with a network environment with other security tools to provide secure IoT device connectivity. The components include the End Node, Gateway, Network Server and Application Server [21]. Figure 2 depicts the LoRaWAN security architecture that incorporates SSL with the TCP/IP that encrypts communication devices such as fire alarms, CCTV cameras, meter, and gas monitoring devices from the end nodes to the gateway routes. The firewall, IPS and TLS are configured on the VPNs and the routers between gateway and network servers to sniff out any suspicious packets. The SSL/TLS and IPS and the external firewalls to secure the Database servers and the cloud services are between the network server and application server. These components are integrated on the LoRaWAN using intelligent devices on the security devices to security configurations and information flows, monitor and establish secure checks.

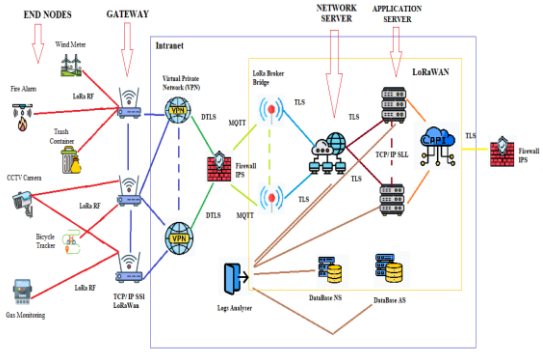

Fig 2. LoRaWAN Security Embedded System

B. *Privacy Protection Issues*

Occasionally sensitive data is stored on devices, such that when these devices connect to a wireless network, they expose passwords and information. Therefore, the devices should oversee sensitive data accurately and safely with an end agreement after each use. Otherwise, an attacker could have access and commit a serious invasion of privacy [22].

C. *Weak and Easy Passwords*

Many interfaces use similar usernames and weak passwords that are easy to guess, such as 'admin'. Many devices have hard-coded credentials issues and few authentic bypass issues. Normally, some users use short passwords or original ones that come with the system. However, when attackers have access to the system as administrators' interface to all the personal data information and change the passwords. [23].

D. *Outdated Software*

Outdated software causes vulnerabilities on IoT devices. Usually, the software is found and fixed automatically using the latest version. However, some vulnerabilities do not allow the system to update and show issues after the device is deployed [24].

IV. IMPLEMENTATION

This section discusses the implementation of the MITM attack on the LoRaWAN. Then, a scenario of an ARP spoofing MITM attack is used to explain how the attack is deployed and how to defend it [28]. Threats to the intelligent devices linked to the LoRaWAN wireless data communication technology have been discovered as the most common assaults using ARP spoofing attacks. Finally, we recommend control mechanisms to prevent ARP spoofing attacks. The goal is to secure user data on IoT devices, which generate a large quantity of information and private information.

A. *Man – In – The – Middle Attack (MITM) Process*

MITM attacker intercepts and interrupts communications between devices and exploits the data between two parties, especially network and application servers. Then, the attacker impersonates either party, stealing data and gathering sensitive information to operate scams or frauds. In a network environment, I.P. addresses communicate, but routers do not as they only use MAC addresses. For instance, computer A asks for the I.P. address of another computer B and C and its MAC address. Once these computers have the ARP cache, they can send messages to each other. To implement the process, we open the power shell and log in as an administrator, then type 'arp-a' to view the static address as the broadcast address to view the computer's arp cache. Next, we type the command 'arp-d' and the computer's I.P. that s sending messages. The entry is deleted. Next, we open Wireshark and ask for the I.P. of 'computer C' and see what it is doing. Then in Wireshark, we type ARP to see with which another computer, 'computer C', was sending messages, as shown in Figure 9. Then the attacker's computer, when it has the message, sends the signals to the router to intervene between the victim's computer and the router.

There are various techniques for launching MITM attacks. The purpose is to gather information to commit scams or frauds. The following are some of the attacks.

I.P. spoofing: the data source is spoofed to fool the victim into thinking there is a genuine conversation [23]

ARP spoofing: poisoning the ARP cache to link the attacker's MAC address to the victim's I.P. address.

DNS spoofing: When an attacker enters the cache and alters the translations to redirect to the DNS domain name system to transform these internet names into easy-to-remember titles. [25] [28] [29].

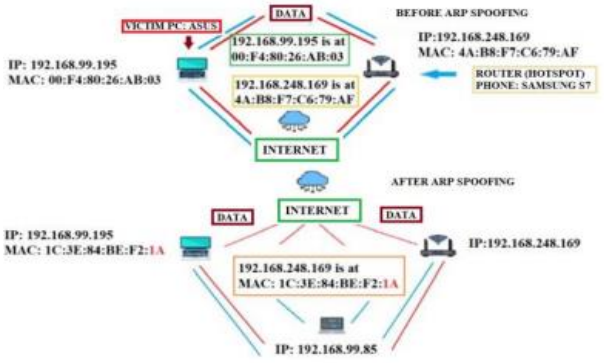

Fig 3. Man-in-the-Middle Attack

The attack demonstrates a lack of security between the web server and the application server. A

MITM attack could lead to more attacks against the user, such as bit flipping attacks. Bit flipping attacks steal data and attempt to change the communication between the network server and the application server, making the LoRaWAN v.1.0 vulnerable network [24]. The type of MITM attack carried out is ARP cache poisoning, by causing the ARP protocol to resolve the I.P. addresses in the networks by poisoning the cache so that the attacker can gain access to information.

B. ARP Cache Poisoning

The ARP Cache Poisoning attack occurs in an event where the recipient's system is required, as the an-ARP request is made. The I.P. and MAC address of the computer makes the request, and the I.P. of the destination computer is provided. This approach aims to provide fake responses to queries so that the user may use the attacker's computer as an access point to the internet and intercept outbound data from the victim's P.C.

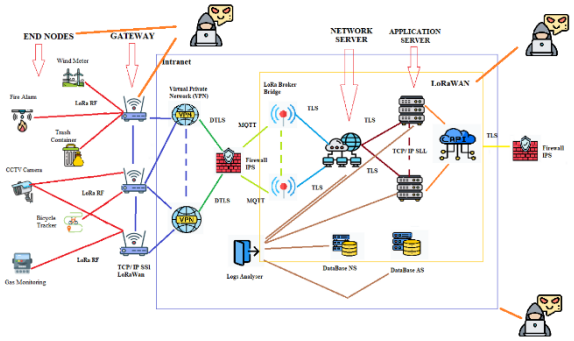

Fig:4. ARP poisoning in each layer

Utilizing the command line may be essential to distinguish that a device's ARP cache has been exploited. We start with the Kali Linx shell as an administrator. We type the following command to show the ARP table on Windows and Linux. Supposed the table contains two specific I.P. addresses with the same MAC address, this demonstrates an ARP assault . Since the I.P. address, 192.168.5.1 can be recognized as the switch, the attacker's I.P. is likely 192.168.5.202. To find ARP spoofing in a huge arrange and get more data around the sort of communication the aggressor is carrying out, you'll be able utilize the open source Wireshark convention.

C. Tools and programmes used

The structure is as follows: Two portals have been utilized to mimic the attack, one of which is a laptop with the Linux operating system installed, which is employed as an attacker and has Kali installed (black laptop, DELL brand). On the other hand, a victim is a laptop using the Windows 10 operating system (grey laptop, ASUS brand). We used a mobile phone hotspot as a network provider for security considerations. Both devices were connected to the same network without constraints. A Wireshark tool was used to analyze the transmission of data and packets. Further, the Ettercap tool in the Linux utility is used to replicate MITM or DoS assaults. The Wireshark assist in detecting failures in the machines that are targeted. It is used as a form of the interceptor (sniffing) to intercept live connections. The implementation starts with the command line in Window (CMD), using the commands "Arp -a," where it is possible to see the ARP catch it and the MAC address for the different devices, hence the default gateway in this MAC. The MAC address is linked to the I.P., and any activity done is sent to the Kali Linux computer. One approach to stop this activity is by carrying out a dynamic ARP inspection; however, if you do not know the type of connection or the type of malicious threat, just a solution is using the protocol message over a local network [25]. The first thing to do is determine the network interface to be utilized, such as the one that provides Wi-Fi access and the I.P. router. In Kali, to access this sort of information, such as the network interface, go to CMD in Start and type Ipconfig, and then the router's I.P. is retrieved by typing I.P. route display (all this is the information from the attacker). Only the victim's I.P. address is necessary and may be found in the CMD or network configuration.

```
C:\Users\Alessandra>arp -a

Interface: 192.168.56.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.248.85 --- 0x11
  Internet Address      Physical Address      Type
  192.168.99.195        4a-b8-f7-c6-79-af     dynamic
  192.168.248.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Alessandra>ip interfaces
'ip' is not recognized as an internal or external command,
operable program or batch file.
```

Fig 5. Checking the Victim Address MAC

After that, we enable packet forwarding in Linux, going to the command line to activate the IPv4 network, the most widely used protocol on internet packages forwarded, where the machine will work as a router. Figure 5 shows how two possible victims were found, considering the ports are the easiest route to access the network and the device to start the ARP poisoning by executing the following command:

"Echo 1 >/proc/sys/net/ipv4/Ip forward" (1)

The command above assists in keeping the flow of communication in the attacker-user path as much as possible and removes the perception of intermediary processing. A second terminal window is used to verify if the MITM attack is operational. Finally, we used the Ettercap tool to gather instant messaging packets automatically and conduct the poisoning of both the gateway and user's ARP.

```
root@TALKTALK9434A7:~# echo > 1 /proc/sys/net/ipv4/ip_forward
root@TALKTALK9434A7:~# ettercap -Tq -M arp: remote /192.168.99.195 / /192.168.99.85/
ettercap NG-0. 7. 4. 2 copyright 2001-2005 ALoR & NaGA

Listening on Wlan0...
  Wlan0 ->     00:F4:80:26:AB:03      192.168.99.100     255.255.255.0
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65531 GID 65533...


  31 plugins
  41 protocol dissectors
  58 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
3492 known services

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 192.168.248.169 00:F4:80:26:AB:03
 GROUP 2 : 192.168.99.195 4A:B8:F7:C6:79:AF

Text only Interface activated...
Hit 'h' for inline help
```

Fig 6. I.P. Forwarding attempt

D. Step to Intercept Packages From The Victim Using An Arpspoof Command

Using this command line allows you to intercept packets on a switched LAN. This works by redirecting packets from a target host on the LAN/WLAN intended for another host on the LAN using ARP replies. Further, we determine if it will be possible to route packets as the device will not receive information from the router. That will show that it is the attacker's computer pretending to be the new router and then be able to sniff the *traffic. arpspoof* of the host to sniff new packets from the command line equivalent. You may choose the network interface to use with the -I command, and with the *-t* command, you can specify which hosts to *spoof. arpspoof* spoofs the MAC address of the host to sniff packets to all hosts on the LAN by default. So the default router is the most common host on a LAN to fake ARP. This step starts with the ARP spoof, and then you must add or choose the target using the victim interface and the I.P. address. Then at the end, add the I.P. address, where we can see the machine starts sending some ARP reply from the computer telling the MAC address of that I.P. The commands used are: *arpspoof -i [Network Interface Name] -t [Victim I.P.] -r [Router I.P.]*

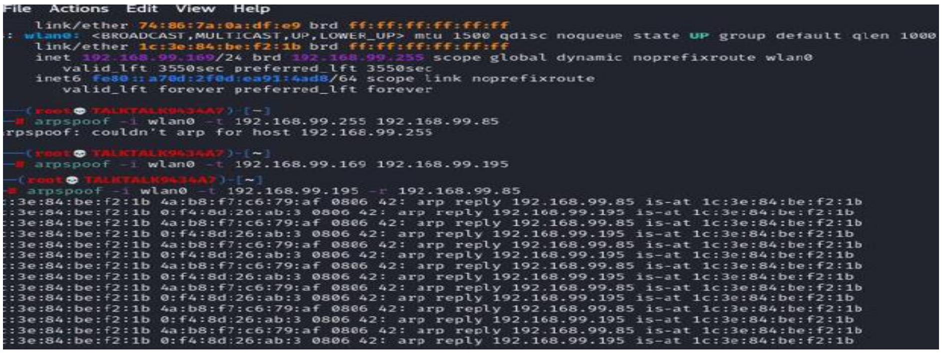

Fig 7. Starting ARP attack on the Victim's Computer

The following step identifies the victim's computer activity to verify that the ARS Spoof attack has been initiated. First, we determine if the MAC address has been changed to the attacker's computer's I.P. address with Kali Linux. Next, we check to see if the changes in the MAC device one have been spoofed, checking the traffic using the *traffic ping 8.8.8.8 command or 192.168.248.28*. Figure 8 shows that the attacker has taken control of the victim’s network, with the packet forwarding verification showing that four packets have been sent and four have been received. That means that none have been lost, and all information received and sent between the two channels is not blocked.

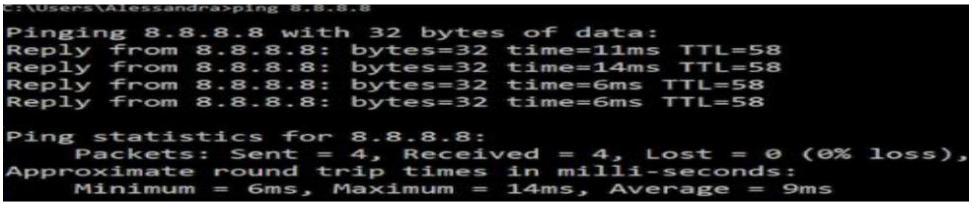

Fig 8. Testing the send and receive packages With the Victim's Laptop

As mentioned above, in the previous step, it is verified that the victim does not lose any packets it sends and receives while being hacked through an ARP spoof attack. After it has been demonstrated that no change has occurred network, the attacker's computer is checked for activity on the victim's control using the Wireshark program. The other way to check is by receiving the traffic from the computer using the Wireshark app, where we will see the information. For example, we could see the attacker's computer was trying to ping the victim's device. The results show that the victim's computer tries to get into the 8.8.8.8 ping command. The attacker can check his traffic because the MAC has been changed from the default gateway, giving all the access to the Kali Linux computer.

At Layer 1101, when the packet is sent from the victim's device to the router, the attacker's poisoned MAC address (instead of the router's original MAC) is inserted as the destination MAC. That is how the packet arrives at the attacker's P.C. The attacker sees this packet and forwards it to the router using the correct MAC address. Logically, the response from the router is sent to the spoofed target MAC address on the attacker's system (instead of the victim's device). The attacker intercepts them and forwards them to the victim's device. Meanwhile, the Wireshark sniffer software running on the attacker's P.C. reads the data traffic, and it is possible to see the control on the victim's computer

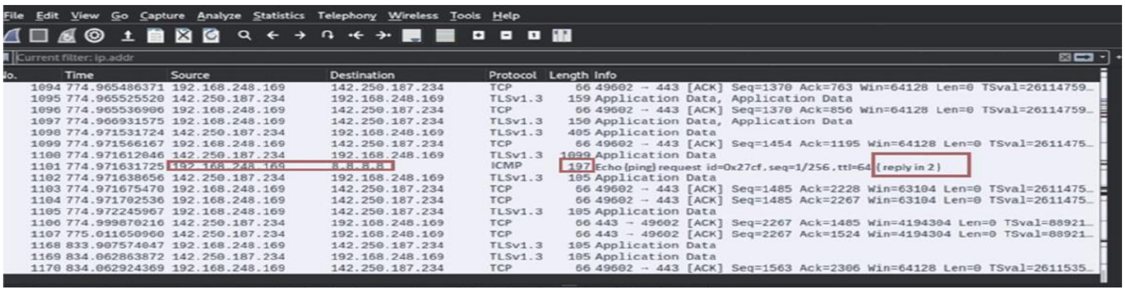

Fig 9. Traffic network of the victim's computer using Wireshark

The next step is to poison the victim's computer with the attack, where we will verify using Wireshark to take control of the devices, and you will see how many times the ARP attack has been sent to the computer. Here we analyze the victim's activity, where you get the different poisoning attacks, which reply every time, the user does anything on the computer. The number of data recorded can be seen here, and how the ARP cache has been turned into ARP packets and is being sent to monitor the target.

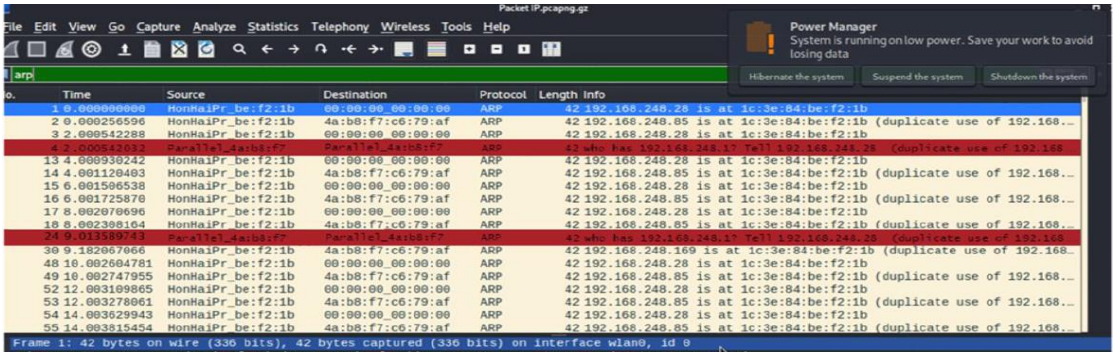

Fig 10. ARP spoof attack detected on Wireshark

E. Sniffing And Testing Using Ettercap Wireshark

Then we sniff and test using the Ettercap Wireshark app to define the type of sniffing Ettercap will do on the various devices in the attacker's networking using a Bridged sniffing method. Once we have a list of hosts, we can start poisoning them with an-ARP assault. The test was performed on a different day but with a separate hotspot. After the packet had been collected and analyzed for traffic utilization, we explored everything from the same port where the victim is connected to determine the websites visited. Then, we can observe the traffic between the target and the destination.

Fig11. Sniffing the Wlan0 and port of the victim's computer

Finally, we demonstrated the final test on the victim's websites to prove that it is possible to get the same result as the victim. We execute the network interface command "*Driftnet -I"* to sniff the network from the HTTP query command line. Figure 9 shows how we can view all the activities by analyzing all the images from TCP streams.

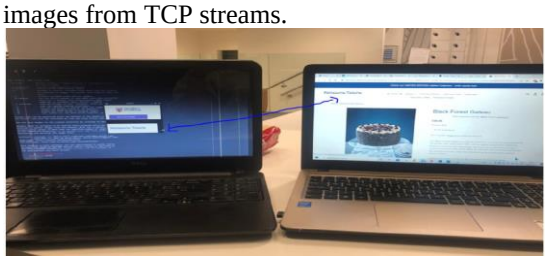

Fig 12. Demonstrate Drifnet Command on the victim's device

V. DISCUSSIONS

ARP Spoof and DNS Spoof are a type of MITM attacks that could be deployed on LoRawWAN, and on the DHCP and ICMP services that oversee the assigning of I.P. addresses and the ARP. In a network environment, the ARP is used to determine the MAC address associated with a given I.P. address. An ARP request for an I.P. address is sent to devices whose MAC address could be identified. The device with the I.P. address responds with an ARP Reply to the MAC address of the devices that made the request. When reviewing the ARP reply, the IoT device stores the IP-MAC address pair locally in an ARP cache table. After the ARP resolution, data is finally sent to the destination. The ARP protocol lack authentication schemes since any device could claim the ARP request. Cyber attackers can deploy ARP Spoofing attacks by exploiting this vulnerability and respond to the ARP request. The I.P. establishes association during resolution with the MAC and then updates itself on the ARP cache to provide access to the attacker. However, there are warning signals that the victim is being targeted. Unexpected or frequent disconnections indicate that it is possible to disconnect users from the system to intercept their passwords or usernames when they attempt to log in again [26]. Thus, connecting to a public or unknown Wi-Fi is insecure and could lead to attackers taking control of the victim's devices.

F. ARP Spoofing Preventive Controls

This section discusses the various security controls that can be implemented as recommendations to prevent ARP spoofing. The LoRaWAN architecture has several security issues when connected to IoT devices. The following control mechanics can be implemented to mitigate attacks on IoT devices.

Static ARP Tables: deploying statically mapped network's MAC addresses to the appropriate I.P. addresses provides the feasibility of control and prevents attacks. That ensures that any network modifications will necessitate manual updates to the ARP cache tables on all the hosts. Monitor duplicate occurrences of the same MAC address on the LoRaWAN. Further, switch security could be implemented as one of the roles for mitigating these ARP attacks as it provides a dynamic ARP check. That validates each ARP message and filters out packets that may be dangerous or suspicious to the system. This inspection form may route messages through a switch to avoid DoS attacks and activate ports using the DHCP snooping capability. Furthermore, physical Security could be implemented to ensure that ARP messages are

not sent beyond the borders of the local network, which means that those who wish to hack into the network must be close to the victim's network or have authority over the computer. Moreover, a VPN tunnel could be connected to the internet through the internet service provider (ISP). Install SSL to ensure HTTPs encrypt the messages and the firewall to detect any malicious attack. The encryption helps to encrypt the user's location and prevents attackers from deploying ARP spoofing attacks. Password management and multifactor authentication could be used to monitor user activities. Additionally, apply zero trust principles to prevent zero-day attacks.

VI. CONCLUSION

Digital transformation, research and innovation advancements in IoT technology has given people with physical and visually impaired hope of a quality of life. These developments have allowed users to access IoT devices and provide ease of use of their everyday household devices for health monitoring, T.V.s, smartphones, computers, pets, doorbells, and CCTVs.

However, these devices are susceptible to attacks and exploitable, posing many challenges to users. Attackers deploy MITM attacks to intercept, interrupt, and modify communications between devices. Detecting and preventing MITM attacks on IoT devices for visually impaired users has been challenging as attackers deploy various methods to exploit the victims on the IoT network. Existing literatures have considered various implementations and recommendations to improve security. This paper has identified multiple attacks that are being deployed on the devices. Further, we have implemented a MITM attack on LoRaWAN using open-source tools and attack commands to identify vulnerabilities in LoRaWAN architecture. Finally, control mechanisms have been recommended to improve security.

Future works will consider Smart City Technology and IoT security exploits on people with disabilities from a distributed cloud environment.

REFERENCES

[1] K. Somasundaram, K. and Selvam, "IOT–attacks and challenges." IJETR, 2018. 8(9), pp.9-12. **10.31873/IJETR.8.9.67**

[2] J. Salazar, and S. Silvestre, "Internet of things". European Virtual Learning Platform for Electrical and Information Engineering, 2017. ISBN 978-80-01-06232-6.

[3] D. Serpanos, and M. Wolf, "Internet-of-things (IoT) systems: architectures, algorithms, methodologies." 2017. Springer. **10.1007/978-3-319-69715-4**

[4] P. Sethi, and S. R. Sarangi, "Internet of things: Architectures, Protocols, and Applications." Journal of Electrical and Computer Engineering, 2017. Doi. **10.1155/2017/9324035**

[5] A. Yeboah-Ofori, J. Abdulai and F. Katsriku "Cybercrime and Risk for Cyber Physical Systems: A Review." International Journal of Cyber-Security and Digital Forensics. IJCSDF. 2019. Vol. 8 No.1. Pg. 43-57. http://dx.doi.org/10.17781/P002556

[6] D. Sobnath, I.U. Rehman, and M.M. Nasralla, "Smart Cities to Improve Mobility and Quality of Life of the Visually Impaired." In: Paiva, S. (eds) Technological Trends in Improved Mobility of the Visually Impaired. EAI/Springer Innovations in Communication and Computing. Springer, 2020. Cham. https://doi.org/10.1007/978-3-030-16450-8_1

[7] M. M. Nasralla, "Sustainable Virtual Reality Patient Rehabilitation Systems with IoT Sensors Using Virtual Smart Cities". Sustainability. 2021, 13, 4716. https://doi.org/10.3390/su13094716

[8] P. Biswajit, "An overview of LoRaWAN" WSEAS Transactions on Communications, 2020. Doi.**10.37394/23204.2020.19.27**

[9] K. L. Tsai, F. Y. Leu, L. L. Hung, and C. Y. Ko, "Secure session key generation method for LoRaWAN servers" 2017.Taiwan: IEEE. Doi:**10.1109/access.2020.2978100**

[10] G. A. Abdalrahman and H. Varol, "Defending Against Cyber-Attacks on the Internet of Things," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6, **10.1109/ISDFS.2019.8757478**

[11] A. Tabassum and W. Lebda, "Security Framework for IoT Devices Against Cyber-attacks" 2019. Doha: IEEE, **10.5121/csit.2019.91321**

[12] M. Ingham, J. Marching and D. Bhowmik, "IoT security vulnerabilities and predictive signal jamming attacks analysis in LoRaWAN". 2019. IET. **https://doi.org/10.1049/iet-ifs.2019.0447**

[13] R. Badhwar, "Man-in-the-Middle Attack prevention." In: The CISO's Next Frontier. 2021. s.l.:s.n., pp. 223-229, 10.1007/978-3-030-75354-2_27

[14] I. Lee, "IoT cybersecurity: Literature Review Adopt Cyber Risk Management" 2020. MDPI. **https://doi.org/10.3390/fi12090157**

[15] P. P. Lopez, J. C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "Attacking RFID Systems" ISM Handbook, 2016. V5. 6th Edition

[16] M. G. Martini, C. T. E. R. Hewage, M. M. Nasrall and O. Ognenoski "QoE Control, Monitoring, and Management Strategies." Kingston University, U.K. Chapter 7. Wiley. 2016. Multimedia Quality of Experience (QoE).

[17] I.U. Rehman, D. Sobnath, M. M. Nasralla, M. Winnett, A. Anwar, W. Asif, and H. H. R. Sherazi, "Features of Mobile Apps for People with Autism in a Post COVID-19 Scenario: Current Status and Recommendations for Apps Using A.I. Diagnostics" MDPI. 2021, 11, 1923. https:// doi.org/10.3390/diagnostics11101923a

[18] I. U. Rehman, M. M. Nasralla, A. Ali and N. Philip, "Small Cell-based Ambulance Scenario for Medical Video Streaming: A 5G-health use case," 2018 15th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), 2018, pp. 29-32, doi: 10.1109/HONET.2018.8551336.

[19] S. B. A. Khattak, M. J. M. Marey, M. M. Nasralla, Q. Guo, X. Gu, "A Novel Single Anchor Localization Method for Wireless Sensors in 5G Satellite-Terrestrial Network" Alexandria Engineering Journal, Volume 61, Issue 7, 2022, Pages 5595-5606, https://doi.org/10.1016/j.aej.2021.11.061.

[20] S. Naoui, M. E. Elhdhili and L. A. Saidane, "Enhancing the security of the IoT LoRaWAN architecture," International Conference on Performance Evaluation and Modelling in Wired and Wireless Networks. (PEMWN), 2016, pp. 1-7, 10.1109/PEMWN.2016.7842904

[21] S. M. Billah, V. Ashok, D. E. Porter, and I. V Ramakrishnan, I. V. "Ubiquitous accessibility for people with visual impairments: Are we there yet?" In SIGCHI 2017. Conference Human Factors in Computer Systems (pp. 5862–5868). New York, NY: ACM. https://doi.org/10.1145/3025453.3025731.

[22] Y. W. Kwon, "A search system to identify vulnerable IoT devices." The journal of the Korean institute of communications and information sciences, 2019. 44(4), pp. 736-742, 10.7840/kics.2019.44.4.736.

[23] X. Jiang, M. Lora and S. Chattopadhyay, 2020. An experimental analysis of security vulnerabilities in industrial IoT devices, s.l.: ACM., https://doi.org/10.1145/3379542.

[24] A. K. Singh, and N. Kushwaha, "Software and hardware security of IoT." s.l., 2021.IEMTRONICS. 10.1109/IEMTRONICS52119.2021.9422651.

[25] J. Nagamalai, S. Banthia,and A. Sharma, "Security in IoT devices" 2021.: IGI Global, 10.4018/978-1-7998-5348-0.ch017.

[26] J. Petters, "What is a man in the middle attack: detection and prevention tips." 2020. [Online] Available at: https://www.varonis.com/blog/man-in-the-middle-attack [Accessed 15 June 2022].

[27] J. Dofe, J. Frey, and Q. Yu, "Hardware Security Assurance in Emerging IoT Applications, 2016. Durham: IEEE. Doi: **https://doi.org/10.1109/ISCAS.2016.7538981**

[28] J. Thomas, S. Cherian, S. Chandran, and V. Pavivithran, "Man in the middle attack mitigation in LoRaWAN" 2020.Amritapuri: ICITC, 10.1109/ICICT48043.2020.9112391

[29] A. Mallik, A. Ahsan, M. M. Z. Shahadat, and J. C. Tsou, "Man-in-the-middle-attack: Understanding in simple words." International Journal of Data and Network Science, 2019.3 (2), pp. 77-92. 10.5267/j.ijdns.2019.1.001.