International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 02 | Feb – 2026 DOI:10.55041/ISJEM05445
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

# Detect Man-In-The-Middle Attack using ARP Analysis

**Mr. Rohan Gurav[1],**

M.sc.IT, Student, Department of Information Technology,
University of Mumbai, India.

and

**Mr. Jayesh Shinde[2],**

Professor, Department of Information Technology,
University of Mumbai, India.

**Abstract:**
In the era of 20s of advanced network and communication. There were lots of devices, applications, web pages, web applications, and IoT devices that connect using some networks and communicate through some "HTTPS, HTTP, URL, UDP, FTP" via different ports. But now we have a network easily, like some SIMs and some free WIFI with 4G and 5G speed.
These wifi networks are easily accessible in shops, restaurants, hotels, railway stations, airports, and even hospitals. However, non-technical people get easily hacked by the attacker.Attackers target the common person using simple tools like HETTY, BETTERCAP, PROXY.PY, BURP, and ETTERCAP. To safe use of free internet and public wifi, we will analyze some network traffic here and periodically monitor the network. Many Python-based tools exist, such as WIRESHARK, but non-technical users may find it challenging to understand properly. Here ,we are using machine learning with Python libraries, particularly "Scapy." to identify and monitor some unwanted and unnecessary network traffic to secure device networks.
***Keywords:*** Machine Learning, Wi-Fi, Wireless Attack, Man-in-the-Middle, MITM, Network, Traffic, Package, Live Detection, Network Monitoring, Serve.

## 1. INTRODUCTION

Now, wireless LAN networks are currently very popular and are expanding quickly. In both rural and urban areas, these networks are growing rapidly and becoming more sophisticated in both small and large organizations. Wireless LANs have a number of advantages over traditional LANs, such as cost and mobility savings. Anyone can set up a wireless network because they are inexpensive and easy to establish. Wireless networks are connected to devices such as computers, telephones, printers, tablets, and other wireless-enabled devices.

These days, the majority of wireless LAN networks are built on IEEE 802.11 standards.
However, as WLAN networks become more common, they lead to various types of attacks due to the many security flaws in this standard. Hazards, vulnerabilities, and threats have increased recently due to the increase of wireless networks.
Because the wireless network is broadcast, any device within its coverage area can transmit and receive data. Because of this, wireless network security is particularly important. However, they can also be exploited by attackers to take advantage of vulnerabilities, threats, botnets, and flaws in the network. There are many in-network attacking techniques that can be used to disrupt your network and pirate your privacy. DDoS, DOS, sniffing, spoofing, and MITM are attacks on work in the network to distract you, pose a danger to your privacy, and disturb your machine.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 02 | Feb – 2026 DOI:10.55041/ISJEM05445
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

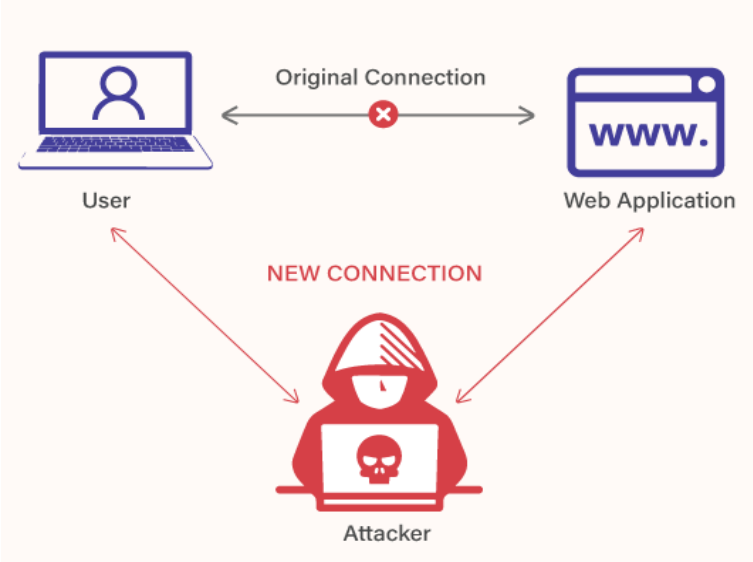


Figure 1: MAN-IN-THE-MIDDLE ATTACK

**A. TYPES OF MITM ATTACK:**

MAN-IN-THE-MIDDLE ATTACK is not a particular single attack; there are huge families to work in MITM. Their various attacks are performed in MITM. They come to various attacks of the group to find vulnerabilities.

*a. IP SPOOFING:*

Similar to DNS spoofing, IP spoofing involves the attacker rerouting internet visitors intended for a trustworthy internet site to a phoney one. The attacker modifies the malicious web page's IP address of the malicious web page to appear as though it is the IP address of the legitimate website visitors were meant to visit, instead of spoofing the domain's DNS record.

*b. DNS SPOOFING:*

Domain Name System (DNS), in-attack DNS chase poisoning, and spoofed DNS entries result in an escalation of actual website traffic to be diverted as malicious or fake traffic to the spoofed website. Just as in all spoofing techniques, the objective is to lure the victims to log in to the spoofed website and make them believe that they want to target and click an action; just as if they are paying a charge or sending the money to an account.

*c. ARP CACHE POISONING:*

ARP (Address Resolution Protocol) is a protocol that is located in the link layer of the OSI model. The rule of ARP is to reconcile one IPv4 address to the MAC address of the device on a local area network. When a device connects with the help of an IP address, ARP reconciles the MAC address of the device, which gives permission for data to be delivered at the link layer level.

*d. SECURE SOCKET LAYER HIJACKING:*

Too many websites use SSH certificates to show secure servers. HTTPS stand as "HYPERTEXT TRANSFER PROTOCOL SECURE". The URL which starts with HTTP, or HTTPS Hypertext Transfer Protocol Secure is mostly used by the browser to access the webpage securely and safely.When the user enters the website in HTTPS, that user uses the secure website and shares documents securely. SSL and successor transport layer security (TLS) are protocols to use in security between computer network layers. In SSL attacks, the attacker intercepts all data passing between a server and the user's computer.

*e. WI-FI EAVESDROPPING:*

WIFI eavesdropping involves sniffing information from unsecured public WIFI; this attack is also known as the "Evil Twin" attack, where the attacker connects the targeted WIFI to the user, and sniffs the user's credentials, monitors network traffic, and captures useful confidential information. This attack is involved in a Man-in-the-Middle (MITM) attack.

**B. TOOLS TO PERFORM MITM:**

*a. ETTERCAP*

The Ettercap tool is open source and also used to find IP Addresses who connect to the same wifi network. This tool performs MITM Attack to perform MITM and some other attacks. The tool widely uses some networks, hosts, and protocols. It is capable of registering network packets in LAN and different settings.

*b. HETTY:*

This tool is too fast and high performance with a quick workflow. This tool is an open source tool which safely supports security research and group projects.With the help of an attacker toolkit, it can be used responsibly for bounty research and network testing. The tool is lightweight and can also manage HTTP traffic, acting as a central proxy to handle Next.js or other web interfaces.

*c. BETTERCAP:*

Bettercap has become the go-to for network security testing because it's essentially a diversified Swiss Army knife. It handles everything from Wi-Fi and BLE to standard IPv4/IPv6 scanning, whether you are on a red team engagement or just doing a bit of reverse engineering. It is most helpful with the 'active' side of testing, like sniffing credentials, DNS spoofing, or capturing handshakes to crack later.

*d. MITMPROXY:*

Mitmproxy is an open-source tool, free to use, easy to install, with multiple utilities and functions, where available consoles and also GUI for web interaction. Get real time data, also can we check HTTP and HTTPS Traffic check also request and responses, also they run in browser local host:8080 and install in CA certificate. Additionally, Mitmproxy allows us to edit headers, replay flows quickly, check custom behavior using Python, making it a perfect tool for developers to check APIs and perform security testing workflows.

*e. BURPSUIT:*

Burpsuit is the most powerful tool to perform web penetration testing and check for wireless attack, this tool to help to research or find loopholes in websites, this tool is a proxy tool to connect client side to server side. Lots of scale and more functions are available with this tool, Every attacker can use this tool at the beginner level.

## 2. LITERATURE

Justice Owusu Agyemang, Jerry John Kponyo, and Isaac Acquah, 2019, In research paper, they have presented lightweight and real-time MITM detection, which specifically uses an algorithm that can be implemented on a WiFi-enabled platform. The algorithm works by first detecting the IP and MAC mappings of the client nodes connected to the gateway. To make things smoother, they have applied Asynchronous Method Dispatch (AMD). They have implemented an algorithm concerning CPU utilisation, detection rate, and network performance.

Chandramohan Sudar, Arjun SK, Deepthi L R, 2017 , In research, they showed that it is primary to keep our Wi-Fi safe, as today's generation is the internet generation; everything depends on the internet. If the password is not complex, it cannot be easily phished or brute forced. They have proposed a WIFI authentication system that generates time-based one-time passwords (TOTP) to keep WIFI networks safe. And create complex passwords. In this system, the user will enter the username and password to log in. The time steps are kept under a minute to allow the users to quickly access the generated TOTP from a trusted device.

Eiman Al Neyadi, Shaima Al Shehhi, Ameera Al Shehhi, Noora Al Hashimi, Mohammad Qbea'H, and Saed Alrabaee, 2020, this work, we are testing public wifi to check security using Raspberry Pi and Kali Linux. By performing some attacks like DNS spoofing, Wi-Fi password cracking, the man-in-the-middle attack, and the evil twin, we find vulnerabilities to prevent. Use a VPN for strong encryption, use a Secure Sockets Layer connection, do not connect to any public Wi-Fi, turn off Wi-Fi when going to public places and not needed, and protect your device by using antivirus. and upgrade daily.

Sheng Gong, Hideya Ochiai, and Hiroshi Esaki, 2020, describe KRACK, which is each of the WiFi hacks also known as channel-based man-in-the-middle attack methods. This is a new method to reliably repeat WPA-2-protected Wi-Fi frames. They have used a new technique to detect channel-based man-in-the-middle attacks, i.e., scan-based self-abolition detection (SSAD). There, any tool does not require a Wi-Fi access point; its entire purpose is for devices like smartphones and IoT devices. SSAD successfully detected and prevented the channel-based man-in-the-middle attack in all 7 places

with an average success rate of 99%, while the original WPA connected to the fake access point. 80% were detected in each place.

Farouq Aliyua, Tarek Sheltamia, and Elhadi M. Shakshukib (2018), This study proposes workload due to the use of multiple IoT devices for cloud services. Grows rapidly, which can lead to an increase in the response time of cloud services and an extension of the response time applications of IoT. To reduce this response time, computing devices should be installed at the edge of the network, close to the user. They have proposed two systems that detect the man-in-the-middle attack at the fog layer. An IDS will check the system regularly; if anything suspicious happens, it will detect it. An IPS ensures that the data is sent securely. IPS is an easy way to detect MITM, eavesdropping, packet modification, wormhole attacks, etc.

Argha Ghosh & A. Senthilrajan, 2020, This work introduces man-in-the-middle attacks by giving examples and case studies. The man-in-the-middle attacks are classified into six techniques: spoofing MITM attacks (like ARP spoofing, ICMP spoofing, DNS spoofing, and DHCP spoofing), TSL/SSL (Secure Socket Layer) MITM attacks, cookie hijacking, BGP (Border Gateway Protocol) MITM attacks, man-in-the-browser, and wireless MITM. In this paper, they have used the deep packet inspection technique to monitor and detect network traffic to manage network bandwidth. This paper shows methods for detecting MITM attacks using (DPI) deep packet inspection and (DFI) deep flow inspection. DPI method or DFI method library for network traffic identification and packet filtering of incoming network traffic.

Tae-Ho Cho and Garam-Moe Jeon's research paper solves the problem of security by combining the time synchronisation one-time password (OTP) and the interlock protocol. In this proposed method, before sending any data, including OTP authentication for the detection of attackers. This experiment demonstrates that both methods have up to a 46% detection rate. This method's prevention success rate is 54% higher than that of other interlock protocols.

Rajinder Singh and Satish Kumar, 2019, In a report paper, they proposed an algorithm to detect attacks. 1) Reason Code 2) Mac timestamp To detect a de-authentication attack, use the criteria of the MAC timestamp of de-authentication packets in the wireless network and their reason code. This algorithm is an established radio-tap header, which analyses to identify whether there is a deauthentication attack on the client side or not.

Gokul Anand and Sahaya BeniJeon's research Prathiba, Gunasekaran, and Gunasekaran (2018), In the study, to monitor the traffic on the Wi-Fi network using AirMon-ng, this tool is capable of monitoring the entire Wi-Fi network. It also analyses packets to use Wireshark and uses the MAC address of the target. The name of the model proposed is an IP-spoofed MITM detector. They have proposed a new solution where data is generated on the fly, which, upon being subjected to a statistical significance test, detects the live attack.

Farouq Aliyu, Tarek Sheltami, Ashraf Mahmoud, Louai Al-Awami, and Ansar Yasar, “Detecting”, 2021, In a research paper showing FC (fog computing) and its wireless node to connect IoT, this technique is shown to enhance the performance of the network and social media. This paper also shows the detection and prevention of MITM using IDS. IDS is an intrusion detection system to detect network activity. This result is 95%.

Ames Jin Kang, Kiran Fahd, Sitalakshmi Venkatraman, Rolando Trujillo-Rasua, and Paul Haskell Downland, 2019, This research paper shows IoT is becoming famous day by day. We use all smart devices for various applications. With more security since IoT devices consist of very sensitive information like IP and MAC addresses, attacks like man-in-the-middle attacks are common for IoT devices. In this paper, they have shown some special nodes so that data can be safely transferred. These nodes do three steps in determining the secured route within the network and avoiding suspicious nodes.

K. V. V. N. L. Sai Kiran, R. N. Kamakshi Devisetty, N. Pavan Kalyan, K. Mukundini, and R. Karthi, 2020, In the present paper. Wi-Fi security, then focusing SBC and Wi-Fi modules to find these fake APs in the air. The result was that the proposed methodology prevented the attack in all scenarios.

Shu-Hung Lee, Yeong-Long Shiue, Chia-Hsin Cheng, Yi-Hong Li, and Yung-Fa Huang, 2022, This study explains about data storage and is completed by the exchange of network information about things. Hence, security is more important in IoT. (DDoS) attack means a denial of service attack. This paper proposes a two-dimensional convolutional neural network (CNN) to detect the affected data servers in IoT as well as attack mode. The result shows it has 99.5% accuracy for two-dimensional CNN and 99.8% for packet traffic. The experiment successfully shows the difference between normal data and affected data.

Jerry John Kponyo, Justice Owusu Agyemang, and Griffith Selorm Klogo, 2020 ,This study analyzes that endpoint man-in-the-middle attacks are a well-known threat to computer security. This attack mainly targets computer networks. Attacker targets destroy the communication between two victims and can perform active or passive monitoring. This mainly affects the integrity of packet flow. In research, they discussed the method to detect EP MITM. The technique is

on the basis of the address resolution protocol (ARP). They have used ML classification models for more accuracy. The method has 99.72% accuracy for the detection of attacks.

Abdulaziz A. Alsulami, Qasem Abu Al-Haija, Ahmad Tayeb, and Ali Alqahtani, 2022, This article reviews that IoT has rapid growth due to its benefits in business. industries, and daily device use. There are important techniques to share about Iot handling safely. This paper discusses machine learning models to demonstrate, detect and classify the attacking modes or activities. It differentiates network traffic into five categories: normal, Mirai attack, denial of service (DoS) attack, scan attack, and man-in-the-middle (MITM) attack. The five models were implemented and used to detect the attack as well as the network activity. These five models are shallow neural networks (SNN), decision trees (DT), bagging trees (BT), k-nearest neighbour (KNN), and support vector machines (SVM). The learning models were implemented on the IoTID20 dataset. Accuracy-deep feature technology model was used. The detection has 99.4–99.9% accuracy.

Sura Abdulmunem Mohammed Al-Juboori, Firas Hazzaa, Zinah Sattar Jabbar, Sinan Salih, and Hassan Muwafaq Gheni, 2023, In this project we have studied how physically connected devices may always be affected by attackers. They have used different machine-learning algorithms to prevent and protect every physical device from attacks by obtaining a dataset from the "Kaggle Website" for MITM or DoS attacks. After getting the dataset, this research applied a preprocessing technique like estimation of values because they contain lots of null values. Here they demonstrate machine learning algorithms to detect and analyse attacks. 1) Random Forest (RF) 2) Extreme Gradient Boosting (XGBoost 3) Gradient Boosting (GB) 4) Decision tree (DT) To evaluate performance, many classification metrics are used, like "precision, accuracy, recall, and f1-score". 1) All algorithms detect MITM with the same performance, which is greater than 99% in all metrics. 2) All algorithms detect DOS attacks with the same performance, which is greater than 97% in all metrics.

Hamidreza Fereidouni, Olga Fadeitcheva, and Mehdi Zalai, 2023, This research paper provides an overview of IoT and its significance. They have discussed the man-in-the-middle attack concept in detail, including their causes, possible solutions, and challenges while detecting and preventing such types of attacks. This paper also shows current issues related to IoT security and investigates some future methods and facilities for improving detection and prevention mechanisms against MITM.

Rajarshi Roy Chowdhury, Sandhya Aneja, Nagender Aneja, Emeroylariffion Abas, 2020.This work for device identification of IoT devices without using their assigned network. They have used fingerprints (DFP) for device identification. DFP identifies the devices with the help of network traffic and radio signals. This identifier is mainly related to hardware and software features to complete the experiment. They have collected some packet "TCP/IP " from this header to identify device fingerprints with the help of original device network packets. To implement this technique, they have used two publicly accessible datasets. They concluded that using the UNSW dataset device, accuracy is up to 97.78%.

Abdelkader Lahmadi, Alexis Duque, Nathan Heraief, and Julien Francq, 2020, In this research paper, we have shown that IoT devices are not only Arduino and Raspberry Pi but also include smartphones, tablets, or PCs. IoT is used in various domains, from smartphones to industrial environments. Also, other technology can try to connect devices, like Bluetooth Low Energy (BLE), which is used to communicate and transfer data. Trivial attacks can easily target this low-security device due to its features and some vulnerability present in its software and communication components. In this paper, they have shown MITM against a BLE (Bluetooth Low Energy) device and collected some datasets of network packet data exchange with and without attack. They have also used machine learning for the detection of this attack by merging unsupervised and supervised techniques. They compared two unsupervised models to reconstruct the model of BLE communications to detect suspicious batches after the text-CNN method to classify the packets as normal or suspicious in each batch. Their result shows accuracy for detection is ≈0.99 and the false rate
(≈ 0.03).

Ana Yacchirena, Darwin Alulema, Darwin Aguilar, Derlin Morocho, Francisco Encalada, and Evelio Granizo (2016), summarizes papers for wireless network systems, WIFI, Snort, and Kismet tools for detection purposes. They have tested the computer security using penetration testing with the Backtrack 5 R3 system, along with tools known as Fern Wi-Fi Cracker and Ettercap to monitor the behaviour of the IDS. After performing the attack, they analysed the result with the help of Wireshark as well, and they also observed how Snort and Kismet were working on it.

Avijit Mallik, 2018,in this study, they have shown how man-in-the-middle attacks work. This attack is a cyberattack where unethical activity entered between two users and also escaped two users. This attack often monitors and changes data that was just realised by two users. The main aim of the paper is to help the readers familiarise themselves with the concept of man in the middle of an attack.

Thuc D. Nguyen, Duc H. M. Nguyen, Bao N. Tran, Hai Vu, and Neeraj Mittal, USA, 2008, this study examines, they have used the method, i.e., the letter-envelope protocol, based on a very hard function to check whether the authentication frame or disassociation frame is from an original user or not. They use 802.11 devices, and the results of the experiment are highly effective against DoS attacks.

Kemal Bicakci, Devrim Unal, Nadir Ascioglu, and Oktay Adalier (2014), This research paper has demonstrated the significance of mobile networks and mobile phone security. Most possible attacks on mobile phones are Man-in-the-Middle (MITM) attacks, and they can be detected without human intervention. They create a mobile ID to provide a cure ID that is authorized by the service provider. They sign up to authorize receiving messages, and smartphones analyze all traffic and attacks, with the alert system provided by the service provider.

Mayank Agarwal, Santosh Biswas, and Sukumar Nandi (2013), This research paper has shown the authentication attack on wifi that they are using IDS (Intrusion Detection System) or IPS (Intrusion Prevention System) technology to check victim presence and finalize lightweight and most accurate with a low false-positive rate.

Stephen Glass NICTA 2009, showed that areas like industries, the health sector, the military, and the public environment mostly use wireless networks. Hence, safety is more important here. These are the people who easily get targeted for the use of wireless networks. This research proposes a mechanism of intrusion detection to detect the attack that will keep the network safe. They have modified the Mac protocol to detect malicious activities. The results from the MAC protocol shows a high detection rate with no false positives and communication.

Abdulrahman Al-Hababi and Sezer C. Tokgoz, 2022 paper showed massive growth on the internet, like social media, streaming, some online app services, etc. All these applications are connected to a network with encrypted network traffic and protect the user's privacy. On the other side, machine learning provides an approach to handling both structured and unstructured data. They give accurate recognition, superior decisions, and a forecast.

## 3. OBSERVATION

We studied some research papers and found some effective techniques there; some are applied mostly in IoT devices. Some techniques and packet analysis protocols help to prevent and detect man-in-the-middle attacks. Not only for Man-in-the-middle attacks but also detect DOS or DDOS attacks. Also found AI and ML techniques to help for the prevention and detection of wireless attacks.

| Detect and Prevent of MITM Using Some Technique | | | | |
|---|---|---|---|---|
| **No.** | **Method** | **IoT** | **ML** | **TOOL** |
| 1 | AMD (Asynchronous Method Dispatch) | IDS for FOG computing | DPI or DFI | Airmon-ng |
| 2 | TOTP (time-based one-time password) | NOS (Network Smartest object) | Reason code<br>Timestamp | SNORT AND KISMET |
| 3 | Some basic techniques (use VPN, Antivirus) | SBC (Single Board computer) | ARP Detect | |
| 4 | SSAD (Self Anonym Detection) | CNN (convolutional neural network) | SNN (shallow neural network)<br>DT (Decision Tree)<br>BT (Bagging Trees)<br>KNN (k-nearest neighbor)<br>SVM (Support Machine) | |
| 5 | Synchronization on OTP | DFP | Random Forest<br>Extreme Gradient Boosting EXG BOOST<br>Gradient Boosting<br>Decision Tree | |
| 6 | MITM-IDS | Text - CNN | Capture Dataset | |
| 7 | Authentication with frame 802.11 device | | | |
| 8 | (IDS), (IPS), (STA) | | | |
| 9 | IDM (Instruction detection mechanism) | | | |

Table no. 01 : Technique and Prevention

This table shows some techniques to detect and prevent MITM. Here is which technique to use to give accuracy about the result.

| Accuracy result about Detection MITM | | | |
|---|---|---|---|
| **REF No.** | **Method/IoT/ML/TOOL** | **Use Technique** | **Result** |
| [4] | Method | SSAD (Self Anonym Detection) | 99% |
| [7] | Method | Synchronization OTP | 48% |
| [10] | IoT | IDS | 95% |
| [14] | Method | MITM-IDS | 89.14% |
| [16] | IoT | CNN | 99.50% |
| [17] | ML | Detect ARP | 99.72% |
| [18] | ML | SNN (Shallow neural network), DT (Decision Tree) BT (Bagging Trees), KNN (k-nearest neighbor), SVM (Support Vector Machine) | 99.4% to 99.9% |
| [19] | ML | Random Forest Extreme Gradient Boosting (EXG BOOST), Gradient Boosting, Decision Tree | 99% |
| [21] | IoT | DFP | 97.78% |
| [22] | IoT | Text-CNN | (≈ 0.99) & false rate (≈ 0.03) |

Table No. 02 Tools and Technique with Result

## 4. CONCLUSION

Research papers show different techniques for securing Wi-Fi networks and detecting or preventing man-in-the-middle attacks.

*a) Detection Techniques:*

papers proposed various detection and prevention techniques for MITM attacks, using some methods like lightweight and real-time detection, TOTP (time-based one-time passwords) for secure authentication, and IDS (intrusion detection systems) at the fog layer to monitor and detect attacks.

*b) Basic safety to follow:*

To increase Wi-Fi security, some research papers suggest using VPNs for encryption, using webpages with a Secure Sockets Layer (SSL) certificate, and avoiding public Wi-Fi. Upgrade your device's software, use antivirus, and turn off your device's Wi-Fi when you are not using it.

*c) IoT Security:*

Increase IoT growth rapidly to secure IoT devices. Some papers suggest some technique NOS (Networked Smart Object) or IDS (Instruction Detection System) to use for fog computing. categories, normal packet track, DOS attack, MITM attack.

*d) Mitigation Strategies:*

some research defines mitigation strategies, means as edge computing using CNN (Convolutional Neural Networks). Also, detect data on the IoT network to create a fake access point using SBCs (single-board computers) and wireless antennas.

***Results:***

Experiment results from various papers showed high accuracy in detecting MITM attacks; the average result shows about 99% accuracy, using various machine learning algorithms and network analysis techniques.

***Machine Learning for Security:***

Machine learning algorithms were used for detecting and classifying attacking modes or activities in IoT networks. These models are different in IoT network traffic and distributed to different

**REFERENCES**

1. Justice Owusu Agyemang Jerry John Kponyo, "Lightweight Man-In-The-Middle (MITM) Detection and Defense Algorithm for WiFi-Enabled Internet of Things (IoT) Gateways," 2019, Vol. 7, No. 1, 1-6 Available online at Published by Science and Education Publishing DOI: 10.12691/iscf-7-1-1
2. Chandramohan Sudar Arjun SK and Deepthi, "Time-based One-Time Password for Wi-Fi Authentication and Security"
3. Eiman Al Neyadi, Shaima Al Shehhi, Ameera Al Shehhi, Noora Al Hashimi, Mohammad Qbea'H, and Saed Alrabaee, "Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux"
4. Sheng Gong Hideya Ochiai, and Hiroshi Esaki, "Scan-based Self Anomaly Detection: Client-side Mitigation of Channel-based Man-in-the-Middle Attacks against Wi-Fi", 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)
5. Farouq Aliyu Tarek Sheltami Elhadi M Shakhshuki, "A Detection and Prevention Technique for Man in the Middle Attack in Fog Computing", The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN2018)
6. Argha Ghos A Senthilrajan, "An Approach for Detecting Man-In-The Middle Attack Using DPI and DFI"Tae-ho Cho and Garam Moe Jeon, "A method for detecting man-in-the-middle attacks using time synchronisation one-time password in interlock protocol-based internet of things"
7. Rajinder Singh, Satish Kumar, "A LIGHTWEIGHT SOLUTION FOR DETECTING DE-AUTHENTICATION ATTACK", International Journal of Network Security & Its Applications (IJNSA), Vol. 11, No. 1, January 2019
8. Gokul Anand Sahaya Beni Prathiba Gunasekaran Ponmani, "Detection of Man-in-the-Middle Attacks in Wi-Fi networks by IP Spoofing", 08 March 2022
9. Farouq Aliyu, Tarek Sheltami, Ashraf Mahmoud, Louai Al-Awami and Ansar Yasar, "Detecting Man-in-the-Middle Attack in Fog Computing for Social Media", DOI:10.32604/cmc.2021.016938
10. James Jin Kang, Kiran Fahd, Sitalakshmi Venkatraman, Rolando Trujillo-Rasua and Paul Haskell Dowland, "Hybrid Routing for Man-in-the-Middle (MITM) Attack Detection in IoT Networks", 978-1-7281-3673-8/19/$31.00 2019 IEEE
11. K. V. V. N. L Sai Kirana, R. N. Kamakshi Devisettya, "Building a Intrusion Detection System for IoT Environment using Machine Learning Techniques", 2020
12. Ruchi Vishwakarma Ankit Kumar Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network", Published online: 29 July 2019 ©Springer Science + Business Media, LLC, part of Springer Nature 2019, Telecommunication Systems (2020) 73:3–25
13. Hitesh Mohapatra[1], Subhashree Rath Subarna Panda2, Ranjan Kumar, Jain Deemed, "Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System", Vol 8, Number 5, May 2020, ISSN 2347 – 3983
14. F. KILINÇER, F. ERTAM and A. ŞENGÜR, "Automated Fake Access Point Attack Detection and Prevention System with IoT Devices", Vol. 8, No. 1, January 2020, ISSN: 2147-284X
15. Shu-Hung Lee, Yeong-Long Shuie, chian-hsin Cheng-Yi Hong and Yung-Fa Huang, "Detection and Prevention of DDoS Attacks on the IoT", Appl. Sci. 2022, 12, 12407. https://doi.org/10.3390/app122312407, Appl. Sci. 2022, 12, 12407
16. Jerry John Kponyo, justice Owusu Agyemnag and griffith Selorm Klogo, "Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach", Vol. 12, No. 3, December 2020
17. Abdulaziz A. Alsulami, Qasem Abu Al-Haija, Ahmad Tayeb and Ali Alqahtani, "An Intrusion Detection and Classification System for IoT Traffic with Improved Data Engineering," Appl. Sci. 2022, 12, 12336.
18. Sura Abdulmunem Mohammed Al-Juboori, Firas Hazzq, Zinah Sattar Jabbar, Sinana Salih, and Hassan Muwafaq Gheni, "Man-in-the-middle and denial of service attacks detection using machine learning algorithms", Vol. 12, No. 1, February 2023, pp. 418–426, ISSN: 2302-9285, DOI: 10.11591/eei.v12i1.4555.

19. Hamidreza Fereidouni, Olga Fadeitcheva, and Mehdi Zalai, "IoT and Man-in-the-Middle Attacks," arXiv:2308.02479v1 [cs.CR] 4 Aug 2023,
20. Rajarshi Roy Chowdhury, Sandhy Aneja, Nagender Aneja, and Emeroylariffion Abashttps://www.fiverr.com/cool_rohan?, "Network Traffic Analysis based IoT Device Identification," BDIoT 2020, August 22–24, ACM ISBN 978-1-4503-7550-4/20/08
21. Abdelkader Lahmadi, Alexis Duque, Nathan Heraief, Julien Francq, "MitM Attack Detection in BLE Networks using Reconstruction and Classification Machine Learning Techniques," Submitted on 24 Sep 2020
22. Ana Yacchirena, Darwin Alulema, Darwin Aguilar, Derlin Morocho, Francisco Encalada, and Evelio Granizo, 2016, "Analysis of Attack and Protection Systems in Wi-Fi Wireless Networks under the Linux Operating System," 9781509011476/16/$31.00 ©2016 IEEE.
23. Avijit Mallik, "MAN-IN-THE-MIDDLE- ATTACK: UNDERSTANDING IN SIMPLE WORDS," Volume 2, Nomor 2, Oktober 2018, 109–134,
24. Thuc D. Nguyen, Duc H. M. Nguyen, Bao N. Tran, Hai Vu, Neeraj Mittal, "A lightweight solution for defending against deauthentication/disassociation attacks on 802.11 networks" Conference Paper • August 2008 DOI:10.1109/ICCCN.2008.ECP.51
25. Kemal Bicakci, Devrim Unal, Nadir Ascioglu, Oktay Adalier, 2014, "Mobile Authentication Secure Against Man-In-The-Middle Attacks," doi: 10.1016/j.procs.2014.07.031,
26. Stephen Glass, NICTA, 2009, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks," 1550-445X/09 $25.00 © 2009 IEEE DOI 10.1109/AINA.2009.131,
27. Abdulrahman Al-Hababi and Sezer C. Tokgoz, 2022, "Man-in-the-Middle Attacks to Detect and Identify Services in Encrypted Network Flows using Machine Learning," 978-1-7281-8704-4/20/