National College of Ireland

Detection of man in the middle attack on fog layer using Intrusion Detection Systems

MSc Research Project
Masters in science cybersecurity

Sri sairam Sivasubramanian
Student ID: x21144761

School of Computing
National College of Ireland

Supervisor: Noel Cosgrave

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Sri Sairam S
Student ID:	X21144761
Programme:	Masters in cybersecurity **Year:** 2022-2023
Module:	Thesis/internship
Supervisor:	Noel Cosgrave
Submission Due Date:	14/08/2023
Project Title:	Detection of Man in the middle attack on fog layer using Intrusion Detection Systems
Word Count: 6594	**Page Count:** 19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Sri sairam S

Date: 13/08/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Detection of Man in the middle attack on fog layer using Intrusion Detection Systems

Sri Sairam Sivasubramanian
X21144761

Abstract

Fog computing, being a dispersed computing architecture, presents advantages, although it also gives rise to security concerns, specifically in relation to Man-in-the-Middle (MITM) attacks. Intrusion detection systems (IDSs) possess the capability to mitigate such hazards. This study aims to detecting Man-in-the-Middle (MITM) attacks inside fog computing systems using IDS. The Intrusion Detection System (IDS) known as Snort is widely recognized in the field. Detection rates of 90% were attained through the use of a testbed that emulated a variety of attack situations, thereby showcasing the proficiency of Snort in accurately recognizing and flagging such malicious endeavours. However, this study highlights many limitations, including the requirement for accurate detection techniques and notable rates of false positives. It is recommended to make alterations to the detection rules of Snort and integrate it with additional security systems to enhance performance. The findings of this research have implications for the future development and enhancement of Intrusion Detection System (IDS) capabilities.

1 Introduction

The Internet of Things (IoT) makes it possible to connect a variety of physical objects, from wearables to simple sensors. Because of this connectedness, intelligent actions may be taken to collect and analyse data from these devices and to offer connected functionality. IoT adoption has completely changed how companies/people manage and use data.
Many businesses are embracing IoT devices and technology, emphasizing how crucial it is to comprehend the security concerns related to IoT. Its widespread application introduces a cutting-edge method that incorporates physical objects into the internet. As a result, cybersecurity threats significantly affect how we live our lives, especially in terms of device vulnerabilities. Critical infrastructure including water treatment facilities, power plants, and transportation networks are all vulnerable, which could have negative societal effects. Additionally, privacy and home security can be violated, making consumer electronics more vulnerable to theft. Due to the vast number of interconnected devices, the limited computing and storage capabilities, the variable battery performance, and the variety of standards and protocols involved, typical security techniques may not be appropriate for safeguarding IoT systems.(Chiang and Zhang, 2016)

To ensure a legal and secure operation of the Internet of Things (IoT), specific security solutions that address the unique problems provided by IoT devices are required. Generic

security methods like firewall, encryption, antivirus etc... may not be adequate to protect the varied range of networked devices and the data they manage.(Roy, Li and Bai, 2022)
The rise of IoT-related services such as smart cities, eHealth, transportation systems, and corporate applications has posed a performance challenge to cloud computing. This difficulty comes because of the unpredictability and frequently high communication delay, privacy concerns, and increased network traffic pressures. The research community has developed the concept of fog computing to address these challenges. Fog computing seeks to address some of the constraints of standard cloud computing by moving cloud service capabilities closer to the network's edge. Instead, then depending entirely on centralized data centers, fog computing decentralizes data processing and storage by distributing it to devices and systems located near data sources, colloquially known as "Things."
Fog computing allows devices such as sensors, embedded systems, mobile phones, and autos to execute some computational tasks locally by extending cloud services to the edge.(Bellavista *et al.*, 2019)

Security in fog computing is becoming increasingly important. Below are some factors that contributes security issues in fog computing:

- Decentralized architecture,
- Data privacy,
- communication vulnerabilities (like MITM). (Ashi, Al-Fawa'reh and Al-Fayoumi, 2020)

A man in the middle attack (MITM) attack is an insider attack in which an attacker intercepts communications between a source node and a target node while both believe they are speaking directly with each other. The hostile internal user impersonates another user on two systems in this type of assault. Eavesdropping and manipulation are the two forms of MITM attacks. Eavesdropping is a passive approach in which the attacker intercepts and listens to transmitted data without modifying it. In an MITM assault including manipulation, on the other hand, the attacker assumes the identity of the original sender and modifies the substance of the transmitted data.(Mallik *et al.*, 2019) There is a strong reason to investigate Man-in-the-Middle (MITM) attacks, which are the most common sort of attack discovered in Fog computing systems.(Stojmenovic and Wen, 2014)

The increased vulnerability of fog computing systems to Man-in-the-Middle (MITM) attacks is due, in large part, to the fundamental architecture of fog nodes, which function as mediators between end devices and the cloud (the "Thing"). Because of this location, the fog architecture is naturally like an MITM attack scenario. In such a scenario, attackers may go unnoticed while abusing the system. Furthermore, fog nodes play an important role in the processing of sensitive data such as health status, medical history, medication records, and other important information such as vehicle speed, destination, and direction. The ramifications of this data falling into the wrong hands might be disastrous.(Khan, Parkinson and Qin, 2017)

Because of the vast and diverse use of nodes in fog computing, implementing typical security mechanisms such as security credentials is challenging, if not impossible. (Chiang and Zhang, 2016)

Aim of the research:

1. **MITM Detection in the Fog Layer** - The goal of this research is to identify MITM attacks in the fog layer.
2. **Lightweight IDS Solution** - Because fog nodes have limited resources, a lightweight IDS is critical.
3. **Energy-Efficient Security methods** - The project seeks to investigate and implement energy-efficient security methods that can provide appropriate detection against MITM attacks while limiting the impact on the energy consumption of the fog node.
4. **Real-Time Detection** - Developing real-time detection capabilities within the lightweight IDS is a vital component of the research.

Limitations:

Accuracy in the Real World - Simulated networks may not accurately replicate the complexity and dynamics of real-world fog computing settings.
Lack of Real-World Attack Scenarios - It may be difficult to accurately mimic real-world attacks and their intricacies in a simulated environment. As a result, the performance of the IDS may not have been adequately evaluated against genuine attack scenarios.
False Positives and False Negatives - Lightweight intrusion detection systems (IDS) may be more prone to false positives (identifying non-attacks as attacks) or false negatives (failing to detect actual assaults).
Attack Sophistication - Advanced tactics may be used by sophisticated attackers to avoid detection by lightweight IDS solutions.

Research Question.
1) How effectively can a security breach be detected by an intrusion detection system in fog layer?
2) How effective is Snort (IDS) in detecting man-in-the-middle (MITM) attacks in fog computing environments?

2 Related Work

To protect the Internet of Things (IoT) from Man-in-the-Middle (MitM) attacks, numerous initiatives have been made. Zhao and Ge (2013) Mutual authentication, communication encryption using symmetric or asymmetric methods, and node isolation are the main strategies used to combat MitM attacks. This method works well in conventional IoT settings however it cannot be applied in fog computing situations. There are currently no recognized industry-wide standards for security or certifications designed expressly to address the security issues posed by fog computing. (Ni *et al.*, 2018)

2.1 Authentication Technique

Liu, Xiao and Chen (2012) suggested an authentication system for the Internet of Things (IoT) that can effectively fight a variety of threats, including key control, replay assaults, eavesdropping, and man-in-the-middle (MitM) attacks. The system takes a strategic approach to achieve this increased security by shifting compute activities to a specialized device known as the Registration Authority (RA). This RA device has significant computational capability and oversees managing the classification and authentication of all linked IoT devices in the network.

Given the context of fog computing, fog nodes are ideally positioned to carry out this activity because they can provide computational resources near edge devices. However, if a fog node is compromised, the entire network may be imperilled. Given that the fog node serves as the central control point, such a breach might provide attackers access to key data and allow them to take control of IoT devices inside the network. As a result, protecting fog nodes becomes increasingly important, mandating the adoption of proper security measures to prevent unauthorized access and potential assaults.Liu, Xiao and Chen (2012)

Stojmenovic and Wen (2014) developed a cloud computing authentication solution that blends public key cryptography with Internet of Things (IoT) technologies. However, because of the high computational and communication overhead, the traditional PKI-based authentication approach becomes unfeasible when used to fog computing (Liu, Xiao and Chen, 2012). As a result, additional approaches for efficiently concealing or minimizing these overheads in fog computing settings are required.

2.2 Behaviour-Based Detection

Mohanapriya and Krishnamurthi (2014) discovered a mechanism to identify grey hole attacks using the Dynamic Source Routing (DSR) protocol. This method is based on a non-cryptographic technique that compares the number of messages sent by a source to the number of messages received by a destination. When receivers detect a difference between these two values, they can notify Intrusion Detection System (IDS) nodes of the presence of a malicious intermediary node. The IDS node then takes measures to isolate the suspect node and alerts other network nodes to the potential threat.
Man-in-the-Middle (MITM) attacks, unlike grey hole attacks, do not delete packets during transmission. Because all packets sent eventually arrive at their intended destination, the strategy described above is unsuccessful in preventing MITM attacks.

The authors proposed using packet arrival time to determine the possibility of an attack in their work Aziz and Hamilton (2009). Detecting an assault along the path is accomplished by comparing the actual arrival time to the projected arrival time. If the difference between the two, referred to as Tdiff, exceeds a specified threshold, an assault is detected.

The use of a defined threshold to identify Man-in-the-Middle (MITM) assaults, on the other hand, may cause difficulties due to the noisy and heterogeneous nature of an IoT network. Because of the variety in packet arrival time, it is difficult to develop a single threshold that successfully recognizes MITM assaults in such an environment.

2.3 MAC-layer-based intrusion detection system

A MAC-based intrusion detection system was created by Glass, Muthukkumarasamy and Portmann (2009), with the main objective of detecting wormhole and man in the middle (MITM) assaults. Wormhole attacks, in which the attacker creates a link between two remote network locations, are an illustration of MITM attacks. According to Pathan (2016), in this type of attack, the source and destination nodes agree on the quantity of frames to be broadcast along with an acknowledgment. As a result, the system identifies an intrusion when an acknowledgment is delivered before the necessary number of packets have been transferred. The researchers showed that the method provides accurate identification, but at the expense of lessening network bandwidth.

2.4 Fingerprinting

According to Faria and Cheriton (2006) signal prints could be used to identify masquerading and resource depletion attacks in wireless networks. Like a wireless device's fingerprint, every wireless device has a distinct signal print. The authors stress that signal prints are challenging to recreate, highly dependent on the client's actual location, and frequently display a similar pattern for packet bursts sent from stationary nodes. The Received Signal Strength Indicator (RSSI) of network nodes is automatically added by the server to the packets to accomplish this detection procedure. The server then compares the received packet's RSSI to the data in its database. The node is labelled as malicious if a particular discrepancy is found.

Differential signal strength was used by the authors to guarantee the system's dependability. However, it is still difficult to fully account for the channel's characteristics, particularly in crowded settings like offices where people are always moving around and interfering with communications.

2.5 Network-based IDS to detect.

Aliyu *et al.* (2021) suggested using signed acknowledgment as part of a network-based IDS strategy to identify wormhole assaults. Challenge-response acknowledgment is the technique, in which the sender sends a message "r" challenging the recipient. The recipient replies by adding a secret value that is normally considered confidential, encrypting it with a key, and producing an acknowledgment packet that is signified by the letters "r,sk." The receiver runs the same calculation with the same variables and compares the results with the acknowledgment packet to determine whether a node is malicious. It is difficult for attackers to carry out unnoticed attacks since each packet's acknowledgment is distinct.

However, the biggest difficulty in putting this strategy into practice is distributing and managing the secret values and encryption keys among all functional nodes in the network. For signed acknowledgment to successfully identify wormhole attacks, this is essential. It requires a trustworthy and effective method to guarantee that each node has access to the proper values and keys without jeopardizing their confidentiality. In order to support big networks with numerous nodes, managing these variables and keys should also be scalable.

Any errors or irregularities in this procedure could result in false positives or false negatives, inaccurate intrusion detection, or both. The system becomes more complex due to the need to ensure that nodes use the appropriate variables and carry out the required computations.

2.6 Artificial Intelligence decision making in Fog computing.

Deep learning-based anomaly and network-based intrusion detection systems (IDS) for the Internet of Things (IoT) were proposed by An *et al.* (2018) and Thamilarasu and Chawla, (2019).

In Thamilarasu and Chawla (2019) the system connects to the network and uses an integrated IDS to conduct data analysis at the transport layer. To gather and process network packets, it makes use of a virtual network client (VNC) module connected to a connection probe. The structured data is then sent into a feed-forward Deep Neural Network (DNN) for intrusion

detection that is constructed using a Deep Belief Network (DBN). Although the system had an accuracy of about 98%, there could be overhead from duplicate packets.

On the other hand, an IDS using a Sample Selected Extreme Learning Machine was proposed by An *et al.*(2018). The technique gathers training samples from fog nodes via the cloud, filters them, and then sends back the most appropriate samples to train the fog nodes. The authors showed that their method produced higher detection accuracy than conventional backpropagation and support vector machine (SVM) techniques.

In Sudqi Khater *et al.*(2019) created an IDS utilizing a single-layer perceptron to track attacks on fog nodes. The system evaluated with Windows and Linux datasets from the Australian Defence Force Academy had a 94% accuracy rate. However, the dataset's reliance on past occurrences raises questions over the system's capacity to fend against attacks on fog nodes in the future.

2.7 Authentication scheme

For the purpose of preventing Man-in-the-Middle (MitM) attacks in fog computing, Rahman et al (2019), suggested a mutual authentication system. To build confidence between fog servers and fog devices, the approach combines the Message Authentication Code with the Advanced Encryption Standard (AES). Key establishment, authentication, and registration are the three steps that make up the algorithm's execution.

All fog servers and users sign up with the control server during registration. Mutual authentication between fog users and servers is required in order to distribute the key. Fog servers and users safely establish the key in a local environment. Despite being simple to build, the algebraic structure does need more computation time.

The following behaviors, according to the research, point to a Man-in-the-Middle (MITM) attack: 1) Modifying packet content; 2) Delaying the arrival of sent packets; and 3) Changing a packet's direction or destination. In order to address this issue, the paper suggests an intrusion detection system (IDS), in which specialized nodes are put within the network to watch the behavior of fog nodes based on the aforementioned criteria in order to spot potentially hostile nodes.

3 Research Methodology

As depicted in Figure 1, the examined distributed fog network comprises two distinct types of nodes in the fog layer: fog nodes (FN) and intrusion detection system (IDS) nodes. The Fog nodes, acting as intermediaries and providing services on behalf of the cloud, receive requests from the IoT nodes. In contrast to cloud services, the proximity of Fog nodes in relation to IoT nodes results in a reduction of network latency. Fog nodes possess the capability to manage intricate tasks and exhibit greater computational capacity in comparison to IoT nodes.

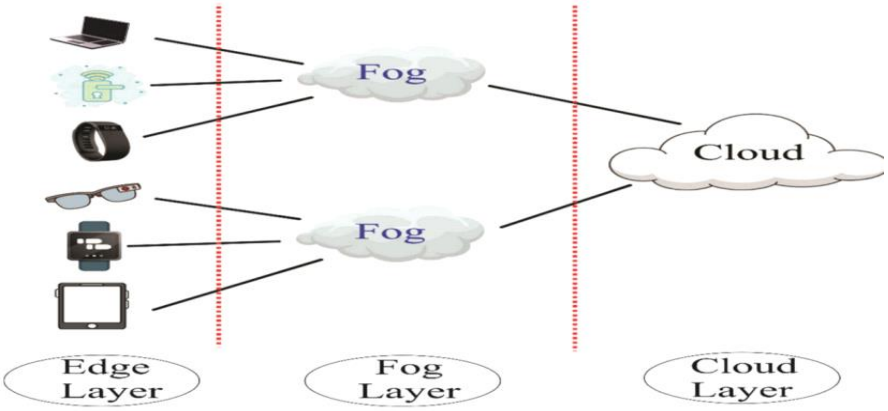

Figure 1 Cloud Computing Architecture

The fog layer serves as a bridge between the IoT and cloud levels, and depending on the design, the details of how it links to each layer may change. For instance, the fog layer could use several communication methods and protocols to connect to the cloud and IoT levels. Though it simplifies the complexity of fog node design, saves energy, and reduces communication lag times by doing away with the requirement for packet format conversion, using the same channel and protocol for communication is encouraged.

The goal of this project is to develop an intrusion detection system (IDS) that can identify Man-in-the-Middle (MITM) attacks occurring within a fog layer.

4 Design Specification

Network Model

The suggested model's application scenario is shown in Figure 2a, where fog nodes gather information from the IoT layer to provide various services to IoT devices. Through a wireless network, these fog nodes are linked together.(Verma and Bhardwaj (2018).

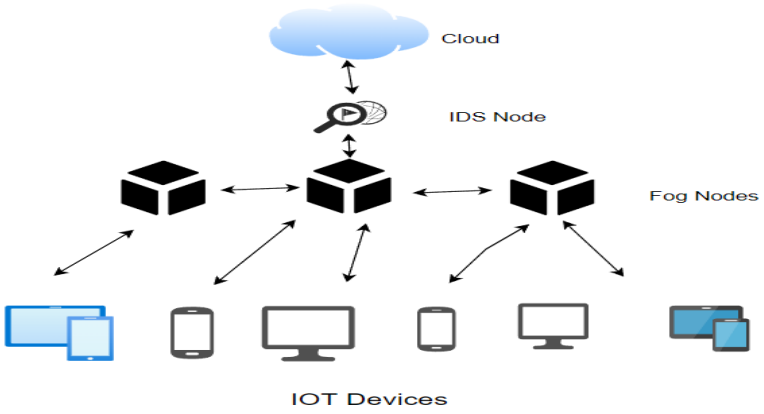

Figure 2a : Application model

The proposed model is simulated using the GNS3 simulator, as shown in Figure 2b. The IDS nodes in this simulation assume the essential responsibility of keeping an eye on the network, spotting potential intrusions, and rapidly alerting other nodes in the network to potential

dangers. The Fog nodes, on the other hand, oversee running and providing services to the IoT layer.

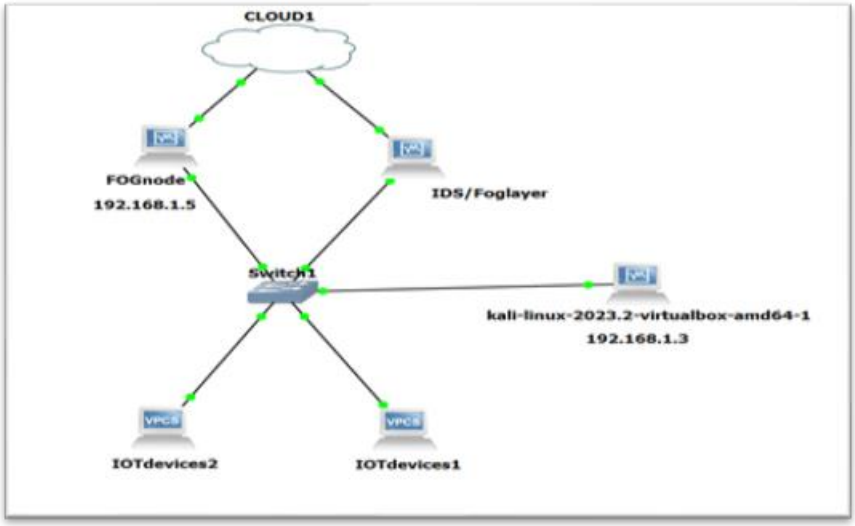

Figure 2b: Proposed simulation model (GNS3)

Attacker Model

The malicious actor in this attacker model conducts a Man-in-the-Middle (MITM) assault inside the fog layer. Attacker focuses on and eavesdrops on packets sent between IoT devices, the cloud, and the fog layer. Even though the attacker may have fewer resources than the cloud, they may still be able to outperform the fog nodes.

Tools used:

NMAP – Used to scan the network and see the open ports.
SCAPPY – Python based tool to redirect ICMP.
ETTERCAP – Launch ARP spoofing attack
Wireshark – To monitor network.

IDS Solution:

The Snort IDS is used in this instance to detect MITM assaults. Snort actively scans the network while functioning as a passive system for any indications of intrusions, attacks, or breaches of security guidelines. The network administrator is instantly notified by the IDS when suspicious events are found. It's crucial to remember that the MITM attack is not directly stopped or prevented by the Snort IDS. Instead, it serves to aid in the successful detection of MITM assaults by offering insightful information about network node activity.

The open-source nature of the software enables modification and facilitates community contributions, resulting in a diverse array of rule sets designed to detect different types of threats. Moreover, Snort's utilization of signature-based detection effectively discerns established attack patterns, while its capability to conduct real-time analysis and packet logging offers proficient network surveillance. The reputation of this solution for intrusion detection is bolstered by its adaptability, active community, and cost-effectiveness.

Evaluation Methodology:

To evaluate the efficacy and dependability of the suggested intrusion detection system for identifying Man-in-the-Middle assaults on the fog layer, a thorough assessment approach is utilized. The selected assessment methodology revolves around the application of a confusion matrix, which is a widely acknowledged and adaptable instrument for measuring the effectiveness of classification systems.

The utilization of a confusion matrix serves as a robust assessment instrument that facilitates a comprehensive examination of classification results. The evaluation of the performance of our intrusion detection system in detecting Man-in-the-Middle assaults within the fog layer is greatly facilitated by the utilization of the confusion matrix, which offers a comprehensive and detailed analysis of the system's accuracy and effectiveness.

5 Implementation

GNS3 Network Topology:

With virtual machines (VMs) standing in for the cloud, IoT devices, and fog layer, set up the GNS3 network topology. To keep them separate from the external network, join all the virtual machines to a host-only network.

Attacker machine (Kali Linux):

As the attacker machine, This author have installed a Kali Linux virtual machine to the GNS3 topology. After that, set the attacker VM's network interface to be on the same host-only network as the other fog layer VMs.

Snort Installation on Fog Layer:

An additional virtual machine added to the GNS3 topology as the fog node where Snort will be set up. Then have Installed Snort on the fog node virtual machine using the package manager provided by the operating system.

Snort Configuration:

Set the Snort IDS listening port to the network interface of the host-only network.
Now Set up Snort to log events and alarms to a particular file for further analysis.

```
# Setup the network addresses you are protecting
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET  s defined in the
# /etc/snort/snort.debian.conf configuration file
ipvar HOME_NET 192.168.1.0/16
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

Pseudo code for IDS

1. Initialize the IDS system with a set of rules that are designed to detect MITM attacks.

2. Monitor network traffic for signs of MITM attacks by analysing the following parameters:
   if packet source or destination IP address is unusual:
      trigger an alert and initiate a response.
   else if packet source or destination MAC address is unusual:
      trigger an alert and initiate a response.
   else if packet timing characteristics indicate packet interception or redirection:
      trigger an alert and initiate a response.
   else if protocol-specific parameters indicate unusual behaviour:
      trigger an alert and initiate a response.

3. If any of the monitored parameters indicate a potential MITM attack, trigger an alert and initiate a response.

4. The response may involve one or more of the following steps:
   if attacker's IP address or MAC address is known:
      block traffic from that address
   else if secure tunnel or VPN is available:
      redirect traffic through the secure tunnel or VPN
   else if TCP connections or DNS queries are affected:
      reset the affected connections or queries.
   else:
      notify the system administrator or security team of the attack and provide detailed information about the incident.

5. Continuously update the IDS system with new rules and monitoring techniques to improve its ability to detect and respond to MITM attacks.

Create MITM Detection rule.

Snort rule to recognize man in the middle attacks.

Start Snort IDS:

With the custom rule active, launch the Snort IDS on the fog node VM.

Generate MITM Attack:

From the Kali Linux attacker machine, launch a Man-in-the-Middle attack. To eavesdrop on communication between IoT devices and the cloud, we can employ attacks like ARP spoofing in fog layer.

Monitoring and Detection:

The fog node VM's Snort IDS logs and alarms can help in checking the MITM attack. The MITM attack should cause an MITM conflict, which Snort should recognize and report as such.

Testing and Tuning:

This researcher have Perform controlled tests with various MITM attack scenarios to validate the accuracy of the Snort rule.

6 Evaluation

Experimental setup:

The GNS3 simulator was utilized to replicate the network topology. Each virtual machine (VM) is configured to use a host only adapter and is connected to each other through a switch. In addition, each workstation was equipped with an additional adapter that facilitated Network Address Translation (NAT) for Internet configuration purposes.

Various types of adapters, such as the bridging adapter, were tested for the virtual machines. However, discrepancies were observed. When a virtual machine (VM) is configured with a bridged adapter, it is integrated into the host system's local network, allowing it to communicate with other devices connected to the same network. As a result of careful consideration, This author have made the decision to utilize a Host-only adaptor.

Dataset description:
The dataset employed in the evaluation was generated via a sequence of manual man in the Middle (MITM) assault scenarios executed by the researchers. (Javeed and MohammedBadamasi (2020)

IDS Effectiveness:

Normal Traffic
In this scenario, the fog computing environment functions under typical circumstances without any ongoing malicious intrusions. The objective is to create an initial stage allowing authentic connection between the fog layer and Internet of Things (IoT) devices. The Intrusion Detection System (IDS) should effectively and accurately classify this network traffic as legitimate and avoid from generating false alerts.

Single MITM Attack
The present scenario involves the execution of a solitary Man-in-the-Middle (MITM) assault inside the circumstances of a fog computing environment. The purpose of the attack is to intercept and manipulate the network communication that occurs between the fog layer and Internet of Things (IoT) devices. The primary goal of the Intrusion Detection System (IDS) is to identify and signal the presence of an attack, while simultaneously minimizing the occurrence of false negatives efficiently and expeditiously.

Multiple MITM Attack
In the scenario, a series of numerous Man-in-the-Middle (MITM) attacks are conducted concurrently to assess the Intrusion Detection System's (IDS) efficacy in managing a more complex attack environment. The Intrusion Detection System (IDS) should possess the capability to effectively and precisely identify and distinguish various instances of attacks while maintaining optimal performance levels.

Metrics:

In 2006, a paradigm was provided by Frédéric Massicotte and his colleagues for the automated evaluation of Intrusion Detection Systems *Lippmann et al* (2006).

By conducting a thorough examination of the information contained within a comprehensive analysis report in paper, it is possible to determine the quantities associated with the four distinct categories of traffic traces. This facilitates the collection of the true positive and false positive traffic trace percentages, namely the detection rate for correct identifications and the rate of false alarms. The two ratios under consideration are:

$$R_{correct} = \frac{\text{Number of true positive traces}}{\text{Total number of traffic traces}} \quad (1)$$

$$R_{false} = \frac{\text{Number of false positive traces}}{\text{Total number of traffic traces}} \quad (2)$$

Hence, it can be concluded that a reliable and impartial assessment of the impact of an intrusion detection system on MITM attack can be obtained. (Massicotte *et al.*, 2006)

R correct = 6/7 = 85.7 %

R false = 1/7 = 14.3 %

During the experimental evaluation, the Intrusion Detection System (IDS) exhibited a detection rate of man in the middle (MITM) assaults that was effective in 6 out of 7 instances, leading to an approximate detection accuracy of 85.7 %. Among the seven instances of MITM assaults targeting the fog layer, the intrusion detection system (IDS) successfully identified and generated warnings for six of the attacks. Consequently, this facilitated the timely detection of potential security breaches, serving as an early warning mechanism.
Attacks we performed number of times, and it is detected.

Confusion Matrix

Table 1: Confusion matrix

n = 10	Detected No	Detected Yes
MITM ATTACK NO	TN = 2	FP = 0
MITM ATTACK Yes	FN = 1	TP = 7

Accuracy

Accuracy refers to the ratio of accurate predictions to the total number of predictions made. The accuracy of the model can be calculated using the formula: Accuracy = (True Positives + True Negatives) / (True Positives + True Negatives + False Positives + False Negatives). In this case, the accuracy is equal to (7 + 2) / (7 + 2 + 0 + 1), which simplifies to 0.9 or 90%.

The system exhibits a high level of accuracy, reaching 90%, which indicates its proficiency in accurately categorizing instances of MITM attacks, whether they are positive or negative.

Precision

Precision refers to the ratio of accurately anticipated positive observations to the total number of predicted positives.

The precision, calculated as the ratio of true positives (TP) to the sum of true positives and false positives (TP + FP), is determined to be 7 / (7 + 0), resulting in a precision value of 1.0 or 100%.

Achieving of a precision score of 100% underscores the system's capacity to recognize and classify instances of detected Man-in-the-Middle (MITM) assaults accurately and decisively.

Recall

Recall, in the context of classification models, refers to the ratio of accurately predicted positive instances to the total number of actual positive instances.

The recall, also known as the true positive rate, can be calculated using the formula TP / (TP + FN), where TP represents the number of true positives and FN represents the number of false negatives. In this case, the recall is equal to 7 / (7 + 1), resulting in a value of 0.875 or 87.5%.

The system demonstrates a recall rate of 87.5%, indicating its ability to accurately identify a substantial fraction of actual Man-in-the-Middle (MITM) attacks. This ensures that only a limited number of occurrences remain unnoticed.

F1-score

The F1-score is a statistical measure that represents the harmonic mean of precision and recall. This metric is utilized to provide a balanced evaluation between the two measures.

The F1-Score can be calculated using the formula: F1-Score = 2 * (Precision * Recall) / (Precision + Recall). By substituting the given values, we can determine that the F1-Score is equal to 0.933 or 93.3%.

The F1-score, which stands at 93.3%, demonstrates an ideal combination of precision and recall, highlighting the resilience of the Intrusion Detection System (IDS) in effectively detecting MITM assaults with both accuracy and broad coverage.

6.1 Experiment / Case Study 1

The initial experiment involves simulating regular network traffic by transmitting ICMP packets from the attacker system to the fog layer. It is unlikely that Snort would classify this as a harmful activity.

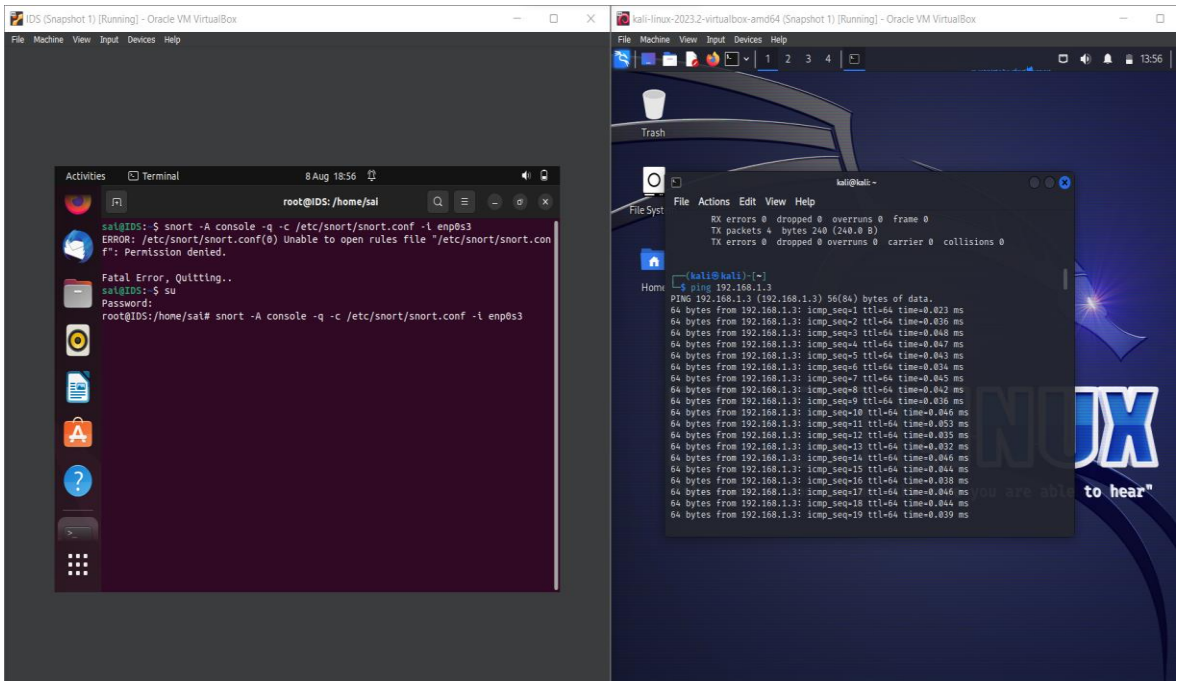

Figure 4 – Sending normal traffic from Kali to Fog layer (IDS permitting the traffic without generating any warning.)

The depicted diagram illustrates the transmission of packets from the attacker machine to the fog layer, with the Snort Intrusion Detection System (IDS) permitting the traffic without generating any warning.

6.2 Experiment / Case Study 2

The current research involves the execution of a single man in the middle (MITM) attack targeting the fog layer, utilizing the Ettercap tool. It is recommended that Snort identifies this incident as a potential man in the middle (MITM) attack.

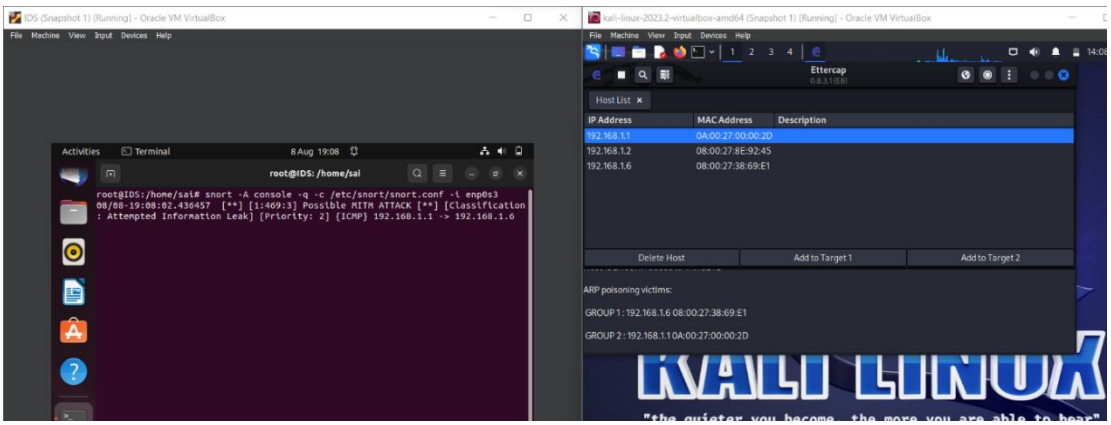

Figure 5: ARP spoofing attack from Kali to fog layer (IDS alerts the traffic as MITM attack

6.3 Experiment / Case Study 3

This case study examines the efficacy of the intrusion detection system Snort through the execution of several man in the middle attacks originating from the attacker's machine. In this scenario, it is expected that the intrusion detection system Snort will successfully detect an identify all instances of attacks.

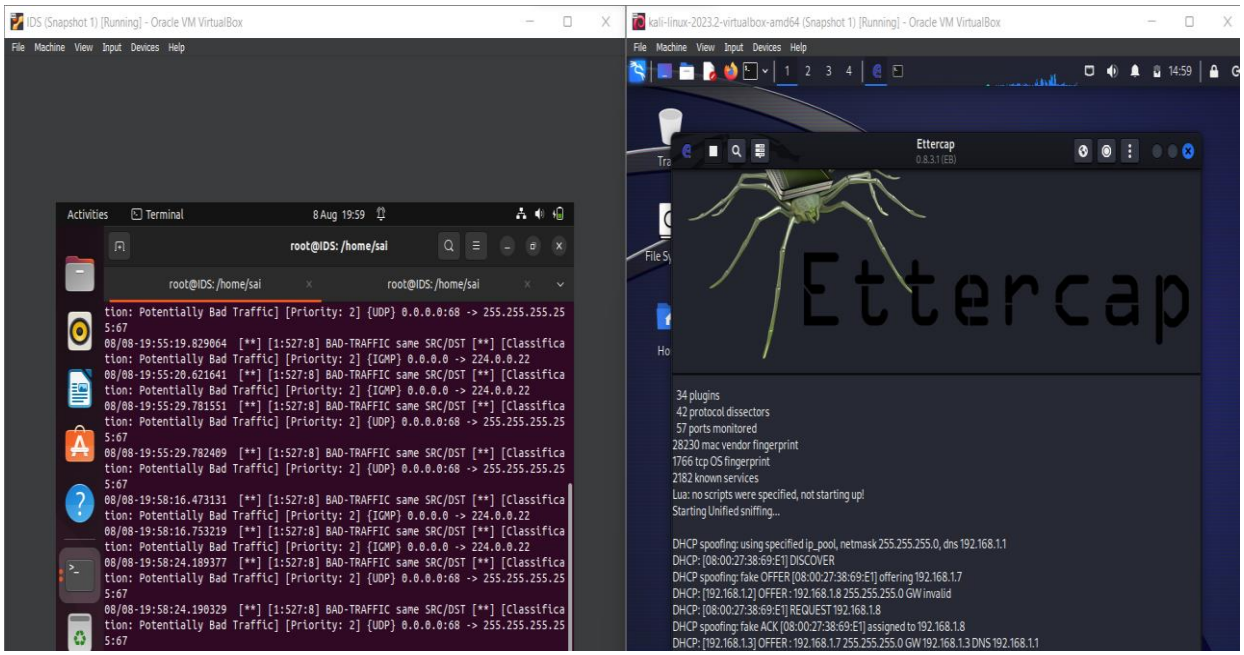

Figure 6: DHCP Spoofing attack (IDS detects the attack)

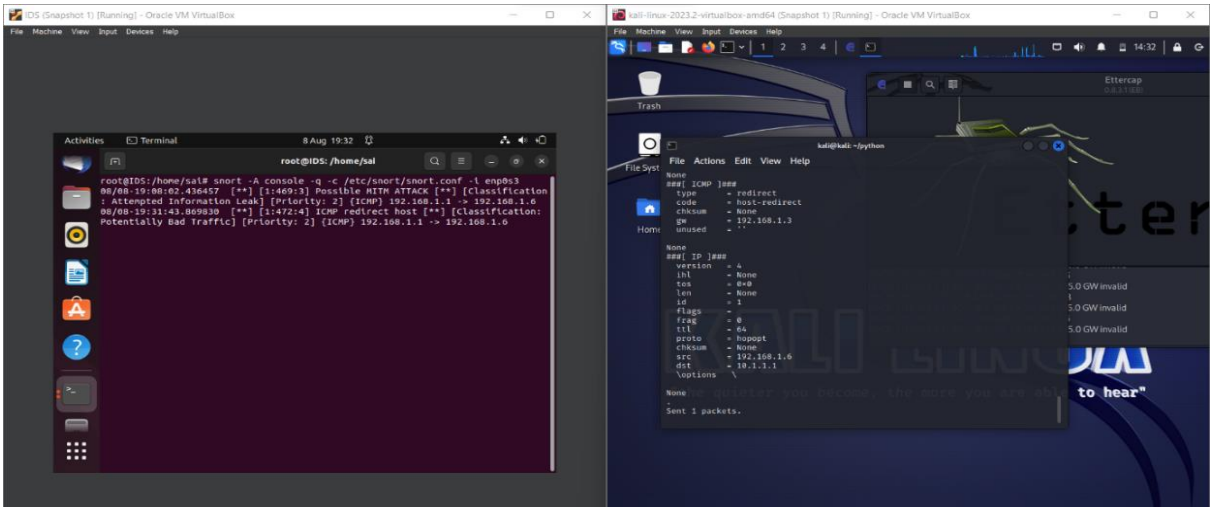

Figure 7: ICMP redirect attack from Kali to fog layer (IDS detects the attack)

6.4 Discussion

This section analyses the Intrusion Detection System (IDS)'s capacity to detect Man-in-the-Middle (MITM) attacks. The effectiveness and limits of this researcher methods are measured by performance. The IDS's 90% MITM attack prediction accuracy shows it can identify good and bad threats. The result verifies the system's evaluation reliability and deployment readiness. Success is a 100 percent precision score. The Intrusion Detection System (IDS)'s pinpoint accuracy detects man in the middle (MITM) assaults. Precision reduces false positives and system disruptions. With 87.5% recall, man in the middle (MITM) attacks were found. This project concludes that the IDS can identify Man-in-the-Middle (MITM) attacks in the scenario. F1-score, accuracy, precision, and recall prove intrusion detection reliability. Upgrade the model to handle evolving attack patterns and network topologies.

7 Conclusion and Future Work

In this research, This author investigated how Man-in-the-Middle (MITM) assaults in fog computing environments can be detected using Intrusion Detection Systems (IDSs), with an emphasis on Snort in particular. Fog computing is becoming more and more popular as a distributed computing architecture, so it is important to make sure that security measures are strong enough to safeguard confidential information and communication channels.

The achieved parameters of accuracy, precision, recall, and F1-score provide validation for the effectiveness of our approach in successfully detecting MITM assaults. The accomplishment serves as both evidence of the efficacy of our strategy and a significant advancement in the establishment of secure communication channels among fog nodes and IoT devices.

This study makes significant contributions to the academic discipline in multiple ways. First and foremost, it tackles a significant security issue in the rapidly evolving domains of Fog Computing and IoT, where interconnection causes vulnerabilities. Additionally, our research emphasizes the capacity of Intrusion Detection Systems to function as dependable protective measures against malicious actions, providing practical knowledge to network administrators.

This study recognizes and understand the inherent constraints and limits present within this author research. The research conducted in our study offers numerous opportunities for further investigation, including expanding the model's relevance to a wider range of assault situations and enhancing resource allocation in larger networks.

Future work

The act of configuring Snort to create alerts, which are subsequently relayed to network administrators or a centralized Security Information and Event Management (SIEM) system, serves to improve network security. The Intrusion Detection System known as Snort is employed to monitor network traffic by utilizing pre-established rules. When a rule is matched with questionable activity, it results in the triggering of alerts. The warnings have the capability to be promptly transmitted to administrators through email or alternative communication channels, facilitating a rapid and efficient reaction. Furthermore, the incorporation of a Security Information and Event Management (SIEM) system facilitates more comprehensive examination by integrating Snort alarms with additional security information, thereby providing context. This methodology enhances proactive identification

of potential threats, facilitates prompt and effective reaction to incidents, and ensures a thorough safeguarding of network infrastructure.

References

Aliyu, F. *et al*. (2021) 'Detecting Man-in-the-Middle Attack in Fog Computing for Social Media', *Computers, Materials & Continua*, 69(1), pp. 1159–1181. Available at: https://doi.org/10.32604/cmc.2021.016938.

An, X. *et al*. (2018) 'Sample Selected Extreme Learning Machine Based Intrusion Detection in Fog Computing and MEC', *Wireless Communications and Mobile Computing*, 2018, pp. 1–10. Available at: https://doi.org/10.1155/2018/7472095.

Ashi, Z., Al-Fawa'reh, M. and Al-Fayoumi, M. (2020) 'Fog Computing: Security Challenges and Countermeasures', *International Journal of Computer Applications*, 175(15), pp. 30–36. Available at: https://doi.org/10.5120/ijca2020920648.

Aziz, B. and Hamilton, G. (2009) 'Detecting Man-in-the-Middle Attacks by Precise Timing', in *2009 Third International Conference on Emerging Security Information, Systems and Technologies*. *2009 Third International Conference on Emerging Security Information, Systems and Technologies*, pp. 81–86. Available at: https://doi.org/10.1109/SECURWARE.2009.20.

Bellavista, P. *et al*. (2019) 'A survey on fog computing for the Internet of Things', *Pervasive and Mobile Computing*, 52, pp. 71–99. Available at: https://doi.org/10.1016/j.pmcj.2018.12.007.

Chiang, M. and Zhang, T. (2016) 'Fog and IoT: An Overview of Research Opportunities', *IEEE Internet of Things Journal*, 3(6), pp. 854–864. Available at: https://doi.org/10.1109/JIOT.2016.2584538.

Faria, D.B. and Cheriton, D.R. (2006) 'Detecting identity-based attacks in wireless networks using signalprints', in *Proceedings of the 5th ACM workshop on Wireless security*. *DIWANS06: Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks 2006*, Los Angeles California: ACM, pp. 43–52. Available at: https://doi.org/10.1145/1161289.1161298.

Glass, S.M., Muthukkumarasamy, V. and Portmann, M. (2009) 'Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks', in *2009 International Conference on Advanced Information Networking and Applications*. *2009 International Conference on Advanced Information Networking and Applications*, pp. 530–538. Available at: https://doi.org/10.1109/AINA.2009.131.

Javeed, D. and MohammedBadamasi, U. (2020) 'Man in the Middle Attacks: Analysis, Motivation and Prevention', *International Journal of Computer Networks and Communications Security*, 8, pp. 52–58. Available at: https://doi.org/10.47277/IJCNCS/8(7)1.

Khan, S., Parkinson, S. and Qin, Y. (2017) 'Fog computing security: a review of current applications and security solutions', *Journal of Cloud Computing*, 6(1), p. 19. Available at: https://doi.org/10.1186/s13677-017-0090-3.

Lippmann, R. *et al.* (2000) 'The 1999 DARPA o€ -line intrusion detection evaluation', *Computer Networks* [Preprint].

Liu, J., Xiao, Y. and Chen, C.L.P. (2012) 'Authentication and Access Control in the Internet of Things', in *2012 32nd International Conference on Distributed Computing Systems Workshops*. *2012 32nd International Conference on Distributed Computing Systems Workshops*, pp. 588–592. Available at: https://doi.org/10.1109/ICDCSW.2012.23.

Mallik, A. *et al.* (2019) 'Man-in-the-middle-attack: Understanding in simple words', *International Journal of Data and Network Science*, pp. 77–92. Available at: https://doi.org/10.5267/j.ijdns.2019.1.001.

Massicotte, F. *et al.* (2006) 'Automatic Evaluation of Intrusion Detection Systems', in *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*. *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, pp. 361–370. Available at: https://doi.org/10.1109/ACSAC.2006.15.

Mohanapriya, M. and Krishnamurthi, I. (2014) 'Modified DSR protocol for detection and removal of selective black hole attack in MANET', *Computers and Electrical Engineering*, 40(2), pp. 530–538. Available at: https://doi.org/10.1016/j.compeleceng.2013.06.001.

Ni, J. *et al.* (2018) 'Securing Fog Computing for Internet of Things Applications: Challenges and Solutions', *IEEE Communications Surveys & Tutorials*, 20(1), pp. 601–628. Available at: https://doi.org/10.1109/COMST.2017.2762345.

Pathan, A.-S.K. (2016) *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. CRC Press.

Roy, S., Li, J. and Bai, Y. (2022) 'A Two-layer Fog-Cloud Intrusion Detection Model for IoT Networks', *Internet of Things*, 19, p. 100557. Available at: https://doi.org/10.1016/j.iot.2022.100557.

Stojmenovic, I. and Wen, S. (2014) 'The Fog computing paradigm: Scenarios and security issues', in *2014 Federated Conference on Computer Science and Information Systems*. *2014 Federated Conference on Computer Science and Information Systems*, pp. 1–8. Available at: https://doi.org/10.15439/2014F503.

Sudqi Khater, B. *et al.* (2019) 'A Lightweight Perceptron-Based Intrusion Detection System for Fog Computing', *Applied Sciences*, 9(1), p. 178. Available at: https://doi.org/10.3390/app9010178.

Thamilarasu, G. and Chawla, S. (2019) 'Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things', *Sensors*, 19(9), p. 1977. Available at: https://doi.org/10.3390/s19091977.

Verma, U. and Bhardwaj, D.D. (2018) 'Security Challenges for Fog Computing enabled Internet of Things from Authentication perspective'.

Zhao, K. and Ge, L. (2013) 'A Survey on the Internet of Things Security', in. *2013 Ninth International Conference on Computational Intelligence and Security (CIS)*, IEEE Computer Society, pp. 663–667. Available at: https://doi.org/10.1109/CIS.2013.145.

Rahman, Gohar & Chuah, Chai Wen. (2019). Man in the Middle Attack Prevention for EdgeFog, Mutual Authentication Scheme. International Journal of Recent Technology and Engineering. 8. 10.35940/ijrte.B1009.0782S219.