MAN IN THE MIDDLE ATTACK IN NETWORK COMMUNICATION

[1]Mrs.K. Nandini,[2]Venkat Sai Emani,[3]Varun Sai Yadla[4]Sri Ram Akkireddy

[1]Assistant Professor, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

knandini.cse@gcet.edu.in

[2, 3, 4, BTech] Student, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301,

venkatsaiemani024@gmail.com,yadlavarun11@gmail.com,sriramakireddy56@gmail.com

ABSTRACT:

In today's interconnected world, network security is of paramount importance to safeguard sensitive information and ensure the integrity of communication channels. Man-in-the-Middle (MitM) attacks pose a significant threat to network security by intercepting and potentially altering communication between two parties without their knowledge. This project aims to develop a MitM detection and alert system to enhance network security. By analyzing Address Resolution Protocol (ARP) requests and responses, the system can detect discrepancies in MAC address mappings, a common indicator of MitM attacks. Upon detecting a potential MitM attack, the system triggers an alert mechanism to notify the affected parties promptly. The alert mechanism includes sending SMS alerts to network administrators or end-users, providing real-time updates on the security status of the network. Additionally, the system incorporates user-friendly interfaces for configuration and monitoring, allowing administrators to customize detection parameters and receive timely alerts on potential security threats. Through the development and deployment of this MitM detection and alert system, the project aims to enhance network security by enabling proactive identification and response to potential MitM attacks, thereby safeguarding sensitive data and ensuring the integrity of network communications

Keywords: Man-in-the-Middle (MitM), communication channels

I INTRODUCTION

This project aims to develop a robust Man-in-the-Middle (MitM) attack detection and alert system, enhancing network security across diverse environments. MitM attacks pose significant threats by intercepting and manipulating communication between parties undetected. This system will employ a combination of network monitoring techniques, including ARP and DNS spoofing detection, along with packet inspection, to identify anomalous behaviors indicative of MitM attacks in real-time. Upon detection, the system will promptly alert network administrators or end-users through various channels, such as SMS messages, enabling swift responses to potential threats. Customizable alert thresholds and automated response mechanisms will ensure adaptability and effectiveness in different network environments. Regular updates and continuous monitoring will be prioritized to keep the system resilient against evolving MitM attack techniques, ultimately bolstering network security posture and safeguarding sensitive data

The main objectives of this project are:

- Detect MitM Attacks: Implement packet sniffing techniques to monitor network traffic and identify suspicious patterns indicative of MitM attacks.
- Real-Time Alerting: Trigger alerts in real-time upon detecting potential MitM attacks. Utilize email notifications and SMS alerts to promptly notify network administrators or end-users about security threats, enabling timely response and mitigation.
- Customizable Alert Thresholds: Provide flexibility in configuring alert thresholds and sensitivity levels based on the specific requirements of the network environment. Allow administrators to customize detection parameters to match the threat landscape and minimize false positives

II. LITERATURE SURVEY

1. Man in the Middle Attacks: Analysis, Motivation and Prevention" Danish Javeed , Umar Mohammed Badamasi , CosmasObioraNdubuisi , FaizaSoomro and Muhammad Asif.Authors-DanishJaveed, Umar Mohammed Badamasi , CosmasObioraNdubuisi , FaizaSoomro and Muhammad Asif.

In The paper discusses Man-in-the-Middle (MITM) attacks in the context of advancing computer systems and applications. It highlights the critical nature of MITM attacks, where an unauthorized third party intercepts and manipulates communication between two users.They categorizes MITM attacks into various types such as Spoofing, DNS Spoofing, DHCP Spoofing, IP Spoofing, and MITM in Vehicular Ad Hoc Networks (VANETs). It also presents simulation results for message delay and message tamper attacks in VANETs.It suggests various detection mechanisms and prevention techniques, including cryptographic solutions, voting-based solutions, server-based solutions, host-based solutions, and hardware solutions.The simulation results indicate that the presence of malicious nodes in a network can lead to delays, packet loss, and compromised messages. They conclude by calling for further research to explore innovative MITM procedures and their impact in different VANET scenarios. They also convey that when ARP cache is accomplished in a dynamic approach, cache entrances can be easily fictitious by counterfeit ARP messages, meanwhile proper verification technique is missing.

2.Security of Cyber-Physical Systems: Design of a Security Supervisor to Thwart Attacks.

Authors- Públio M. Lima ,Marcos V. S. Alves ,Lilian Kawakami Carvalho, Marcos V. Mor

This paper the authors propose a defense strategy against man-in-the-middle attacks in the sensor and/or control communication channels of CPSs modeled as discrete-event systems (DES). They introduce the concept of network attack security (NA-Security), which focuses on preventing the system from reaching unsafe states by using a security supervisor.The proposed defense strategy aims to mitigate damages caused by these attacks without introducing communication delays, which are critical in industrial systems.

The proposed defense strategy involves designing a security supervisor to disable controllable events, preventing the system from reaching unsafe states during an attack. Importantly, this strategy works alongside the existing supervisor, enhancing the system's security without overly restricting its operation.The proposed defense strategy assumes the existence of a pre-designed supervisor and introduces a new security supervisor, which may add complexity to system implementation.

3.A Machine Learning Model for Detection of Man in The Middle Attack Over Unsecured Devices.

Authors- Bilal Ahmad Mantoo and Parveen Kaur.

This paper addresses the security concerns of Internet of Things (IoT) devices, particularly focusing on the increased risk of Man-in-the-Middle (MITM) attacks. And proposes a machine learning-based model for detecting MITM attacks, specifically using the K Nearest Neighbor (KNN) algorithm.The authors collected data using a TP-link gateway connecting multiple devices, simulating MITM attacks through ARP spoofing. The dataset includes features extracted from the packet headers, such as version, length, identification, TTL, and more. The model achieved an accuracy of 98% in detecting MITM attacks based on the selected features.

Main Drawback: The study heavily relies on ARP spoofing for simulating MITM attacks. While this is a common method, other MITM techniques (DNS spoofing, session hijacking) are not considered.

4. **Detecting Man-in-the-Middle Attacks on Non-Mobile Systems**

Authors- Visa Vallivaara

In this paper we propose a method for detecting man-in-the middle attacks using the timestamps of TCP packet headers. From these timestamps, the delays can be calculated and by comparing the mean of the delays in the current connection to data gathered from previous sessions it is possible to detect if the packets have unusually long delays. We show that in our small case study we can find and set a threshold parameter that accurately detects man-in-the-middle attacks with a low probability of false positives. Thus, it may be used as a simple precautionary measure against malicious attacks. The method in its current form is limited to non-mobile systems, where the variations in the delay are fairly low and uniform. The first one requires the users to carry a physical device for authentication and the second one requires all the devices that connect to the server have encryption certificates. History has it that even with the assumption of ideal cryptography, one cannot be assured that the messages will be safely delivered to the intended recipient [6]. This is because even though a security protocol is designed perfectly, security vulnerabilities in the implementation do not cease to exist. Additionally, the ability of users to assure the security of a connection is lacking, due to the complexity of modern networked systems

III SYSTEM ANALYSIS

EXISTING SYSTEM

The existing systems for detecting Man-in-the-Middle (MitM) attacks typically rely on a combination of network traffic analysis, anomaly detection, and signature-based methods. Network intrusion detection systems (NIDS) and intrusion prevention systems (IPS) are commonly used to monitor network traffic for suspicious patterns or known attack signatures. Additionally, specialized tools and software packages, such as Wire shark and Snort, offer packet inspection and protocol analysis capabilities to identify unauthorized access or data manipulation. However, these systems often face challenges in detecting sophisticated MitM attacks, particularly those employing stealthy techniques like ARP and DNS spoofing. Moreover, the reliance on signature databases may limit the effectiveness of these systems against zero-day attacks or novel evasion tactics. Consequently, there is a growing need for more advanced and proactive MitM detection solutions that can adapt to emerging threats and provide timely alerts to network administrators.

Limitations of Existing System

- Limited Detection Capabilities: Traditional network security measures such as firewalls and intrusion detection/prevention systems may not be specifically designed to detect MitM attacks. As a result, they may overlook subtle signs of ARP spoofing, DNS poisoning, or other MitM techniques.

- Reactive Response: Many existing security solutions rely on reactive incident response strategies, meaning they only respond to security incidents after they have occurred. This approach can lead to delays in detecting and mitigating MitM attacks, allowing attackers to remain undetected for extended periods.

PROPOSED SYSTEM

The proposed system aims to enhance MitM attack detection by leveraging a combination of network traffic monitoring, anomaly detection, and real-time alerting mechanisms. It incorporates advanced techniques such as ARP and DNS spoofing detection to identify unauthorized access attempts and data interception activities. The system operates by continuously monitoring network traffic for suspicious patterns indicative of MitM attacks, such as inconsistencies in ARP tables, abnormal DNS resolution behavior, and unauthorized MAC address changes. Upon detecting potential threats, the system triggers immediate alerts to network administrators via email or SMS notifications, ensuring prompt mitigation actions can be taken to secure the network environment. Additionally, the system offers centralized logging and reporting functionalities to facilitate forensic analysis and post-incident investigation, enabling organizations to understand the scope and impact of MitM attacks for proactive security posture improvement. Overall, the proposed system provides a comprehensive and proactive approach to MitM attack detection, helping organizations safeguard their network infrastructure and sensitive data from evolving cyber security threats.

Proposed system Advantages:

- Enhanced Network Security: By continuously monitoring network traffic and detecting MitM attacks in real-time, the system helps organizations strengthen their overall network security posture. It proactively identifies and mitigates threats before they can cause significant damage or data loss.
- Early Threat Detection: The system employs advanced anomaly detection techniques and machine learning algorithms to identify subtle indicators of MitM attacks. By detecting deviations from normal network behavior, it can identify and respond to threats at an early stage, minimizing the impact on network operations.
- Reduced Risk of Data Breaches: MitM attacks pose a significant risk to data confidentiality and integrity. By promptly detecting and mitigating these attacks, the system helps reduce the risk of sensitive data breaches and unauthorized access to confidential information

IV IMPLEMENTATION

Architecture:

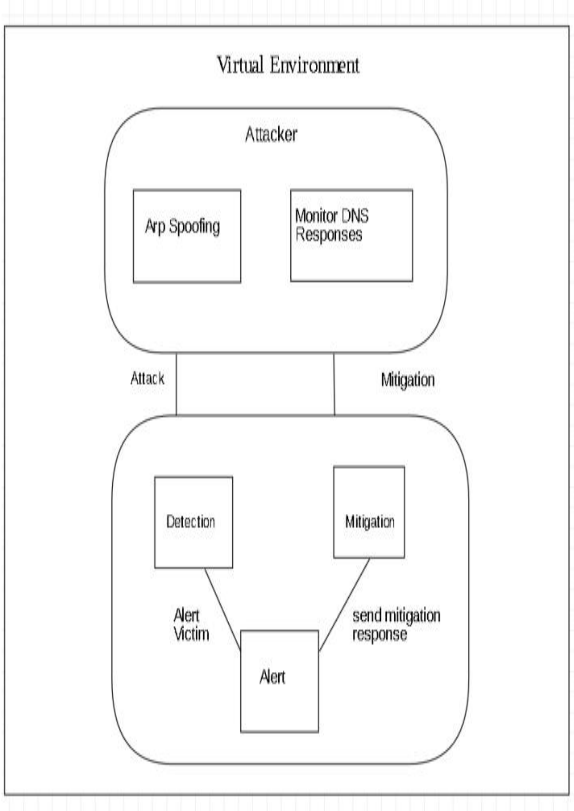


Fig-1. Architectures of the system model

MODULES

Attacker Modules-

ARP Spoofing Module: Responsible for crafting and sending ARP spoofing packets to the victim and the router. It includes functions to construct ARP packets with spoofed MAC addresses and send them periodically to maintain the attack.

Monitoring DNS Responses: This module monitors DNS responses to gather information about the victim's network activity. By intercepting DNS queries and responses, the attacker can gather data about the victim's visited websites and potentially launch further attacks.

Victim Modules-

ARP Detection Module: Detects ARP spoofing attacks by analyzing ARP packets on the network. It includes functions to capture ARP packets, compare them with known network configurations, and raise alerts if inconsistencies are detected.

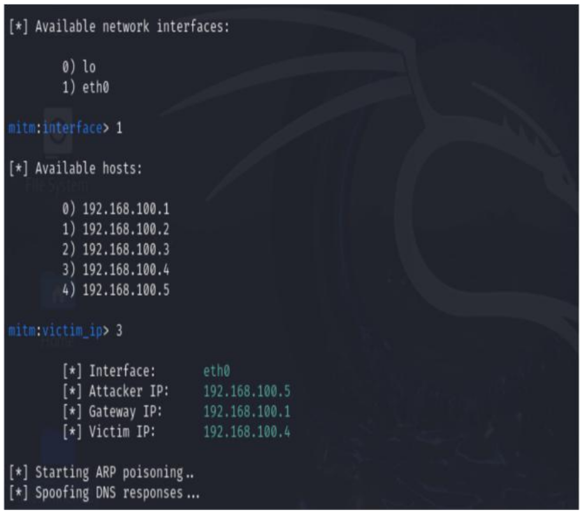
Mitigation Module: Responds to detected ARP spoofing attacks by taking preventive measures to mitigate their impact. This may involve blocking suspicious ARP packets, updating ARP tables, or alerting network administrators about the attack.

Alert Module: Sends alerts to network administrators or users when ARP spoofing attacks are detected. It includes functions to generate and send notifications via email, SMS, or other communication channels to notify stakeholders about the security threat.

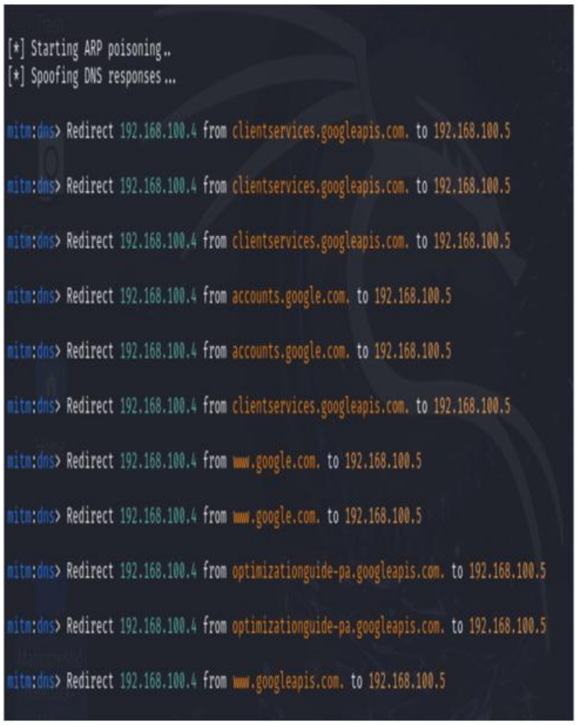
Process:

Implementing a Man-in-the-Middle (MITM) attack detection and prevention system involves several key steps. First, the system needs to be set up to monitor network traffic. This involves selecting the appropriate network interface and enabling IP forwarding on the attacker's machine to facilitate packet forwarding between the victim and the gateway. Once the network is configured, the system continuously monitors ARP and DNS traffic for signs of spoofing or tampering. To detect ARP poisoning, the system analyses ARP requests and responses to identify inconsistencies in MAC addresses, which may indicate ARP cache poisoning. Similarly, for DNS spoofing detection, the system inspects DNS responses for anomalies such as unexpected IP addresses or domain name mismatches. When suspicious activity is detected, the system raises alerts or notifications in real-time, informing the victim about potential attacks. Additionally, the system can perform network traffic analysis to identify other types of MITM attacks, such as packet interception or modification. Machine learning or anomaly detection techniques can be employed to automate the detection of malicious behaviour and patterns in the network traffic. To prevent MITM attacks, the system implements preventive measures such as deploying cryptographic protocols like HTTPS to secure communications. It also educates users about best practices for secure browsing and network hygiene to reduce the risk of falling victim to MITM attacks. Logging and reporting mechanisms are implemented to maintain detailed records of detected incidents, including timestamps and affected parties. Periodic reports are generated to summarize detected threats, vulnerabilities, and mitigation efforts for review and analysis. Continuous monitoring and updates are essential to keep the MITM detection system effective against evolving threats. Regular updates address emerging vulnerabilities and fine-tune detection rules based on real-world observations and feedback. Finally, legal and ethical considerations are taken into account to ensure compliance with privacy laws and regulations while deploying and operating the MITM detection system.

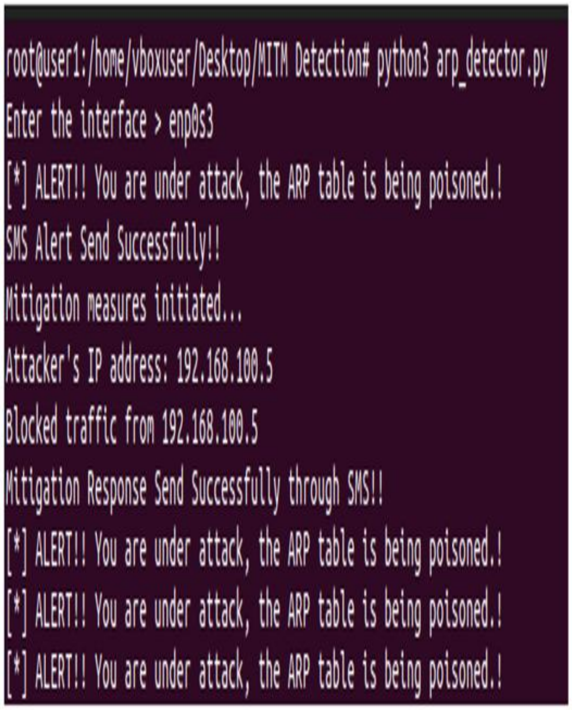
V RESULT AND DISCUSSION



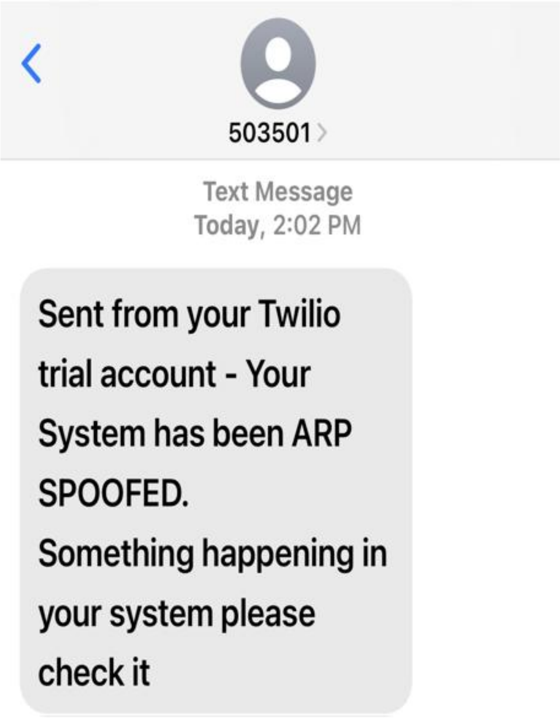
```
[*] Available network interfaces:

        0) lo
        1) eth0

mitm:interface> 1

[*] Available hosts:

        0) 192.168.100.1
        1) 192.168.100.2
        2) 192.168.100.3
        3) 192.168.100.4
        4) 192.168.100.5

mitm:victim_ip> 3

        [*] Interface:      eth0
        [*] Attacker IP:    192.168.100.5
        [*] Gateway IP:     192.168.100.1
        [*] Victim IP:      192.168.100.4

[*] Starting ARP poisoning..
[*] Spoofing DNS responses...
```



```
[*] Starting ARP poisoning..
[*] Spoofing DNS responses...

mitm:dns> Redirect 192.168.100.4 from clientservices.googleapis.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from clientservices.googleapis.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from clientservices.googleapis.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from accounts.google.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from accounts.google.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from clientservices.googleapis.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from www.google.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from www.google.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from optimizationguide-pa.googleapis.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from optimizationguide-pa.googleapis.com. to 192.168.100.5

mitm:dns> Redirect 192.168.100.4 from www.googleapis.com. to 192.168.100.5
```



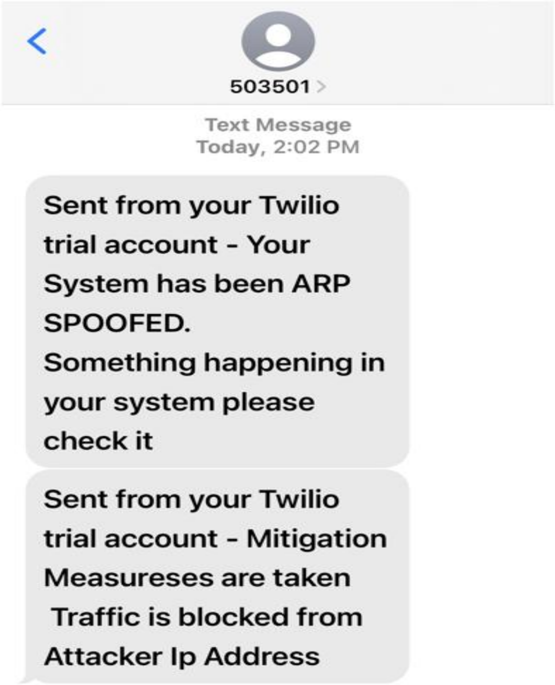
```
root@user1:/home/vboxuser/Desktop/MITM Detection# python3 arp_detector.py
Enter the interface > enp0s3
[*] ALERT!! You are under attack, the ARP table is being poisoned.!
SMS Alert Send Successfully!!
Mitigation measures initiated...
Attacker's IP address: 192.168.100.5
Blocked traffic from 192.168.100.5
Mitigation Response Send Successfully through SMS!!
[*] ALERT!! You are under attack, the ARP table is being poisoned.!
[*] ALERT!! You are under attack, the ARP table is being poisoned.!
[*] ALERT!! You are under attack, the ARP table is being poisoned.!
```



503501 >

Text Message
Today, 2:02 PM

Sent from your Twilio trial account - Your System has been ARP SPOOFED. Something happening in your system please check it



Sent from your Twilio trial account - Your System has been ARP SPOOFED.
Something happening in your system please check it

Sent from your Twilio trial account - Mitigation Measureses are taken
Traffic is blocked from Attacker Ip Address

VI CONCLUSION

In conclusion, the Man-in-the-Middle (MITM) attack detection and mitigation project provides an effective solution for identifying and mitigating potential security threats posed by attackers attempting to intercept communication between two parties. By implementing a combination of ARP detection, DNS monitoring, and response mechanisms, coupled with network interface management and alerting functionalities, the project offers robust protection against common MITM attack vectors. Through the integration of various modules such as ARP detector, DNS monitor, and mitigation scripts, the system provides a comprehensive defense mechanism for safeguarding network integrity and confidentiality. Additionally, the inclusion of features like SMS alerts enhances user awareness and enables timely response to detected threats. Overall, the project demonstrates a proactive approach to network security, empowering users to detect and mitigate MITM attacks effectively.

FUTURE ENHANCEMENT

There are several potential enhancements and further developments that can be implemented to improve the effectiveness and capabilities of a Man-in-the-Middle (MITM) attack detection and prevention system:

1. Enhanced Detection Techniques: Implement machine learning algorithms or anomaly detection mechanisms to identify patterns indicative of MITM attacks more accurately. .

2. Behavioral Profiling and User Authentication: -Utilize behavioral profiling techniques to establish baseline network behavior and detect deviations indicative of unauthorized activities, including MITM attacks.

3. Secure Communication Channels: - Deploy encrypted communication protocols and certificate-based authentication to secure network traffic

VII REFERENCES

[1] M. S. Olimjonovich, "Software Defined Networking: Management of network resources and data flow," 2016 International Conference on Information Science and Communications Technologies (ICISCT), 2016

[2] Nkosi, Mpho, et al. "Classification of SDN distributed controller approaches: a brief overview." 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE). IEEE, 2016.

[3] Brooks, Michael, and Baijian Yang. "A Man-in-the-Middle attack against OpenDayLight SDN controller." Proceedings of the 4th Annual ACM Conference on Research in Information Technology. 2015.

[4] Tunggal, A. What Is a Man-in-the-Middle Attack and How Can It Be Prevented. *UpGuard.com.* Jan 23. 2022 [online] url: https://www.upguard.com/blog/man-in-the-middle- attack

[5] Mallik, Avijit. "Man-in-the-middle-attack: Understanding in simple words." Cyberspace: JurnalPendidikanTeknologiInformasi 2.2 (2019)

[6] ANADIOTIS, Angelos-Christos, et al. SD-WISE: a software-defined wireless sensor network. *Computer Networks*, 2019

[7] FARRIS, Ivan, et al. A survey on emerging SDN and NFV security mechanisms for IoT systems. *IEEE Communications Surveys & Tutorials*, 2018

[8] Nick McKeown, Tom Anderson, HariBalakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. 2008. OpenFlow: enabling innovation in campus networks. SIGCOMM Comput. Commun, 2008

[9] OpenDayLight Project, ‘Platform Overview - OpenDaylight’ [online], Available: https://www.opendaylight.org/ . [Acceses:15 May 2022]

[10] Ettercap Project, Available: https://www.ettercap-project.org/ [Access. 30 oct 2022]

[11] Prasadu Peddi (2015) "A machine learning method intended to predict a student's academic achievement", ISSN: 2366-1313, Vol 1, issue 2, pp:23-37.

[12] Prasadu Peddi (2015) "A review of the academic achievement of students utilising large-scale data analysis", ISSN: 2057-5688, Vol 7, Issue 1, pp: 28-35.

AUTHORS

Mrs. K. Nandini,Assistant Professor Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: knandini.cse@gcet.edu.in

Mr. Venkat Sai Emani, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: venkatsaiemani024@gmail.com

Mr.Varun Sai Yadla, Dept. of CSE-Cyber Security, Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: yadlavarun11@gmail.com

Mr. Sri Ram Akkireddy, Dept. of CSE-Cyber Security,Geethanjali College of Engineering and Technology Cheeryal (V), Keesara (M), Medchal(D), Hyderabad, Telangana 501301.

Email: sriramakireddy56@gmail.com