CYBER THREAT IDENTIFICATION IN OPEN WIFI

Dr. S. SPELMEN VIMALRAJ[1]
Assistant Professor, Department of IT & Cognitive Systems, Sri Krishna Arts and Science College, Coimbatore – 641008[1,3].

Dr. H. VIGNESH RAMAMOORTHY[2], N. KARTHIK[3]
Associate Professor, Department of Computer Application, PES University, Bangalore – 560085[2].

Abstract **- Technology is becoming an indispensable part of modern digital operations due to the increasing reliance on it and the interconnected networks it creates across all industries. In today's world the common cyberthreats seen in open and public Wi-Fi networks include DDoS attacks and impersonation. Data transfer happens when an open Wi-Fi configuration is set up, making it possible to watch attacker launches and victim-targeting spoofing actions. In order to improve security measures, anomalous behaviors are found, categorized, and assessed through security analysis and linked device monitoring. Potential risks are warned of by a warning notification system, and persistent threats are countered and prevented from connecting to the public Wi-Fi network. It explores how to use external threat feeds and repositories to improve the system's threat detection capabilities. It also goes into the field of threat intelligence integration. It aims to increase public Wi-Fi networks' ability to promptly detect and counter emerging cyberthreats by working with industry partners and utilizing worldwide threat information sources. This will fortify the networks' defenses against dynamic attacks. The ultimate goal is to strengthen the security posture overall by developing workable solutions to safeguard user information and privacy in public Wi- Fi areas.**

Index Terms **– DDoS attacks, Impersonation attacks, Cyber threat detection, Cyber Security.**

I. INTRODUCTION

Public/open Wi-Fi networks are intrinsically vulnerable to cyber threats, posing serious risks to users' sensitive information and personal data. One of the most common threats in public Wi-Fi environments is impersonation, where malicious actors pose as legitimate network access points to intercept and manipulate users' data. Attacks known as denial of service (DDoS) involve flooding a network with excessive traffic, which can disrupt services and compromise the availability of the network for legitimate users. Recent years have seen a revolution in connectivity, allowing users to access the internet with unparalleled convenience [3].

This project aims to conduct a detailed research of cyberthreats associated to open and public Wi-Fi networks, with a specific focus on impersonation and DDoS assaults, in recognition of the urgent need to solve these security concerns. Through the identification of gaps and vulnerabilities in the current system, this research aims to create practical solutions that improve public Wi-Fi environments' security posture. As part of the system design, an open Wi-Fi configuration is set up to make data transmission and communication between connected devices easier. The goal of the research is to identify and classify unusual behaviors that could be signs of possible dangers by continuously monitoring device activity and packet movements. The project aims to distinguish between legitimate network activity and malicious conduct by utilizing sophisticated threat detection algorithms and machine learning approaches, so enabling timely intervention and response [5].

- The system employs a warning alerting system as proactive measure to mitigate threats.
- Users will receive timely notifications about any security threats, enabling them to take the necessary steps to safeguard their privacy and data.
- The System aims to protect the integrity and security of the network ecosystem by implementing strong mitigation techniques to prevent harmful entities from accessing the open Wi-Fi network in situations where threats persist or intensify.

The results and suggestions of this project can help develop best practices and standards for safeguarding public Wi-Fi environments through cooperative efforts between researchers, industry stakeholders, and policymakers, ultimately fostering a safer and more secure digital ecosystem for all users [6].

Cybersecurity encompasses the techniques, instruments, and protocols employed to prevent harm, unauthorized entry, and assaults on digital networks, systems, and information. Technology is becoming an indispensable part of modern digital operations due to the increasing reliance on it and the interconnected networks it creates across all industries. Network traffic, system logs, and user activity are continuously monitored and analyzed to promptly detect and neutralize potential threats. Technologies like endpoint protection platforms (EPP), intrusion prevention systems (IPS), and intrusion detection systems (IDS) significantly assist in threat detection and prevention. Organizations value their data, so safeguarding it from theft, tampering, and illegal access is crucial. To protect sensitive data both in transit and at rest, data loss prevention (DLP) technologies, access controls, and encryption are frequently employed. Frameworks for identity and access management (IAM) make guarantee that only those with permission can access particular data and resources on a company's network. The application of multi-factor authentication is involved here [8].

One of the main causes of cybersecurity issues continues to be human error, despite the use of Multi-Factor

Authentication (MFA), identity verification techniques, and role-based access control (RBAC). Therefore, it is crucial to train staff members and end users on security policies, best practices, and typical risks in order to cultivate a security-conscious culture inside enterprises. Even with the greatest of intentions, security mishaps can still happen. Organizations can reduce downtime, quickly recover from assaults, and effectively limit the impact of security breaches when they have strong incident response procedures in place [9].

II. LITERATURE REVIEW

Klogo and Boateng (2020) introduce a lightweight rogue access point detection algorithm for Wi-Fi-enabled IoT devices. The convergence of technologies has led to an intelligent network that connects devices for information exchange, but it also exposes IoT devices to various security risks. As most IoT devices rely on Wi-Fi for communication, they are vulnerable to Wi-Fi attacks, particularly rogue access points. These threats can compromise the security and privacy of connected devices [1].

Asaduzzaman and Majib (2020) explore Wi-Fi frame classification and feature selection to detect Evil Twin attacks. These attacks occur when an attacker masquerades as a legitimate access point, collecting or altering data and potentially stealing user credentials. The study analyzes traffic from both rogue and authorized access points to identify these threats. Their detection method achieved an accuracy of 91.24% [4].

Yan (2022) presents a real-time method for identifying rogue Wi-Fi connections, which are vulnerable to impersonation attacks by devices with identical MAC/IP addresses or SSIDs. Traditional network security techniques struggle to defend against such attacks. The study introduces a novel security approach that detects and rejects rogue Wi-Fi devices or access points (APs) using environment-independent traits from channel state information (CSI). It demonstrates that the nonlinear phase error of subcarriers, due to I/Q imbalance and defective oscillators in Wi-Fi network cards, can be used to identify rogue devices regardless of environmental factors [7].

Jaysankar and Mohan (2023) address the issue of beacon forgeries in Wi-Fi networks, which have become a threat due to the lack of protection on beacon frames. These forgeries can lead to attacks such as de-authentication, DoS, beacon flooding, and WPA2 handshake vulnerabilities. The study proposes a machine learning-based signature detection system to distinguish between authentic and counterfeit beacons. This approach aims to meet the challenges of handling high network traffic and the need for rapid anomaly detection in dynamic network environments [2].

III. EXISTING SYSTEM

The existing approach to detecting cyberthreats connected to open or public Wi-Fi networks is a complex structure with several parts and features designed to maintain connectivity while controlling security concerns. Wireless access points (APs), which are purposefully placed gadgets that provide Wi-Fi connectivity to users inside the network's service area, are the network's fundamental components. In order to provide safe access, these APs use encryption and authentication methods like WPA2 or WPA3, authenticating users and encrypting data transfers to avoid eavesdropping and illegal access [10].

Authentication mechanisms are complemented by intrusion detection and prevention systems (IDPS), which examine network traffic for anomalous activity suggestive of cyber threats. These systems have the ability to recognize anomalies, such as DDoS assaults or rogue access points, and send out notifications for more research or mitigation. One of the most important parts of network security is firewalls. Incoming and outgoing communications must follow pre-established security standards to thwart malware and other online risks as well as prevent unauthorized access attempts [11].

Network monitoring solutions facilitate the discovery of usage patterns, detection of abnormalities, and troubleshooting of connectivity difficulties by giving administrators access into network traffic, device connections, and performance indicators. Security information and event management (SIEM) systems, which gather and analyse security event logs from a range of network devices and applications, facilitate the handling of security.

By teaching users about the proper practices for using public Wi-Fi networks, education and user awareness efforts are crucial for reducing the hazards connected with these networks. using encryption solutions like VPNs, recognizing secure connections, preventing phishing scams, and safely accessing these networks. Frequent security audits and assessments ensure compliance with industry standards and legal requirements, review the effectiveness of the present security measures, and identify areas that require improvement [12-14].

An incident response strategy outlines how to handle security issues like network hacking and data breaches. In order to minimize interruption and data loss, these include incident containment, impact assessment, and the restoration of regular operations.

IV. PROPOSED SYSTEM

In order to improve threat detection, mitigation, and prevention capabilities, the suggested solution for strengthening cybersecurity in public/open Wi-Fi networks combines cutting-edge technology, proactive defensive mechanisms, and user-centric methods. Implementing an advanced intrusion detection and prevention system (IDPS) that is strengthened to efficiently identify known and unknown cyber threats using behavioral analysis techniques and machine learning algorithms is essential to this. Secure network access is achieved by increased traffic encryption techniques and multi-factor authentication systems, which lessen the likelihood of unwanted access and data interception.

Continuous monitoring and integration with threat intelligence feeds enable proactive threat hunting and prompt reaction to new threats, providing real-time visibility into network traffic and security problems. Collaborative defensive mechanisms support cybersecurity best practices and cybersecurity hygiene among Wi-Fi users, whereas user-centric security awareness initiatives coordination of event response and information exchange. Effective incident detection, analysis, and reaction are made possible by an incident response strategy and cyber resilience framework, which guarantees organizational preparedness and flexibility in the face of changing threats. The cybersecurity posture of public Wi-Fi networks is further strengthened by ongoing development and adherence to regulatory compliance requirements, protecting user privacy and data security in today's linked digital environment [15].

IMPERSONATION DETECTION MECHANISMS:

To identify rogue access points and impersonation attempts on the network, the system uses sophisticated approaches. This includes MAC address spoofing, beacon frame analysis to spot abnormalities suggestive of impersonation attacks, and monitoring for illegal Wi-Fi networks with identical SSIDs.

STRATEGIES FOR MITIGATING DDOS ATTACKS:

The system uses distributed denial of service (DDoS) attack mitigation techniques to identify and stop assaults that target public Wi-Fi networks. This entails traffic filtering, IP blacklisting, and rate limitation in order to lessen the effects of volumetric assaults and avoid service interruption.

V. SYSTEM ARCHITECTURE

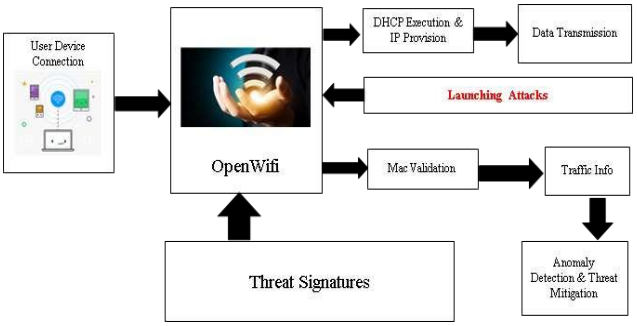


Figure 1 .Block Diagram of Threat Identification

V.1.OPEN WI-FI CREATION

- Thorough preparation had been done to identify the ideal configuration settings, such as SSID, encryption algorithms, and authentication techniques, before the open Wi-Fi network was put into operation.
- A thorough testing step was carried out once the setup settings were determinedin order to guarantee compatibility with a variety of devices and operating systems

2. CONNECTING AND DATA TRANSMISSION USING OPEN WI-FI.

- Users may join their devices to the network by choosing the assigned SSID and completing the authentication procedure once the open Wi-Fi network had been set up. Devices were given dynamic IP addresses by the network's DHCP server after completing the authentication process successfully.
- This allowed them to communicate with other devices and access network resources. Protocols like TCP/IP and UDP/IP have made it easier for data to be transmitted across open Wi-Fi networks, allowing devices to exchange data packets safely and effectively

3. IMPERSONATION ATTACK CREATION

- Thorough reconnaissance had been carried out to find prospective targets and weaknesses in the public Wi-Fi network before the impersonation assault was launched. After completing the reconnaissance phase, the attacker deployed rogue access points (APs) with faked MAC addresses and SSIDs to start the impersonation assault.

- The faked SSIDs were broadcast using methods including beacon frame injection, which tricked unwary users into connecting to the rogue APs rather than the authentic network access points.
- Furthermore, the rogue APs had been disguising themselves as trustworthy devices through the use of MAC address spoofing, which made it difficult for consumers to discern between malicious and legitimate access points.

4.DDOS ATTACK CREATION

- The attacker had identified possible targets within the public Wi-Fi network, including network infrastructure, prior to initiating the DDoS assault. servers, switches, and routers, among other parts. After identifying the targets, the attacker launched the denial-of-service assault (DDoS) by bombarding the targets with a large amount of malicious traffic that was produced by several different sources.
- SYN flood, UDP flood, and ICMP flood were only a few of the DDoS attack vectors used to overwhelm the network infrastructure and impair service availability. In order to increase the impact of the DDoS assault and the amount and intensity of malicious traffic sent towards the targets, the attacker had used botnets or hacked devices**.**

5. ATTACK DETECTION AND MITIGATION

- The intrusion detection system (IDS) had promptly notified network administrators upon detecting unusual behavior within the public Wi-Fi network, therefore initiating a prompt reaction. Sophisticated traffic analysis methods had been used to spot unexpected connection requests, abrupt traffic volume spikes, and anomalous packet speeds that may be signs of impersonation and DDoS assaults.

- Mitigation measures were put in place to stop rogue access points and stop more illegal access to the network after an impersonation attack was discovered. Similar to this, traffic filtering and rate restriction were implemented as soon as a DDoS assault was discovered in order to lessen its impact and restore normal service to the network.

V.ALGORITHM USED

- System performance is evaluated using performance metrics like detection rate and detection latency.
- Detection Rate (DR), commonly known as True Positive Rate (TPR) by the system, isa measurement of the proportion of all real assaults that are correctly recognized.
- Regarding attack detection, delay describes how long it takes the system to identify and react to an assault. In the detecting procedure, an assessment is carried out between Deep Q Learning and Deep Neural Network

DETECTION RATE

It is the ratio between correct detections to the total detections.

$$Accuracy = No\ of\ correct\ Detections / Total\ Detections$$

DETECTION DELAY

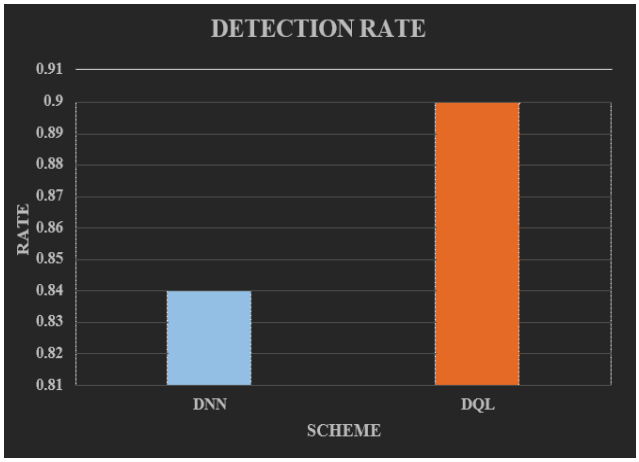
The overall running time for the detection process from the time of attack launch.

$$Detection\ Delay = Detected\ Time - Attack\ Launch\ Time.$$

When a Deep Q-Learning (DQL) and a Deep Neural Network (DNN) model were tested for attack detection, the DQL model showed a better detection rate (0.9) than the DNN model (0.84). This indicates that the DQL model detected 90% of all real assaults, compared to the DNN model's 84% detection, indicating that the DQL model fared better at properly identifying attacks than the DNN model. The findings suggest that the DQL technique could provide a better way to identify harmful activity in cybersecurity applications.

Figure 2. Detection rate for the suggested and current approach

- When a Deep Q-Learning (DQL) and a Deep Neural Network (DNN) model were tested for attack detection, the DQL model showed a better detection rate (0.9) than the DNN model (0.84).
- This indicates that the DQL model detected 90% of all real assaults, compared to the DNN model's 84% detection, indicating that



the DQL model fared better at properly

identifying attacks than the DNN model. The findings suggest that the DQL technique could provide a better way to identify harmful activity in cybersecurity applications.

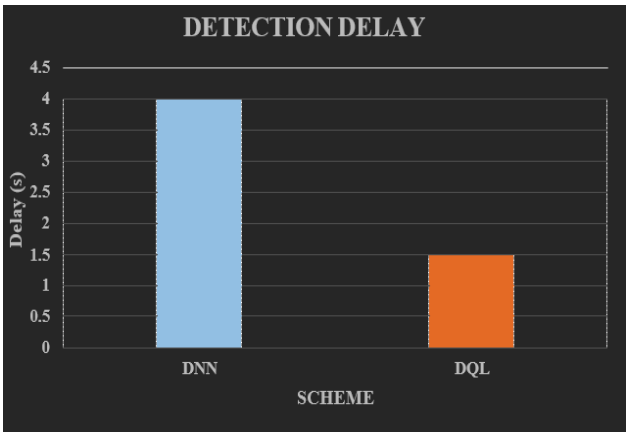
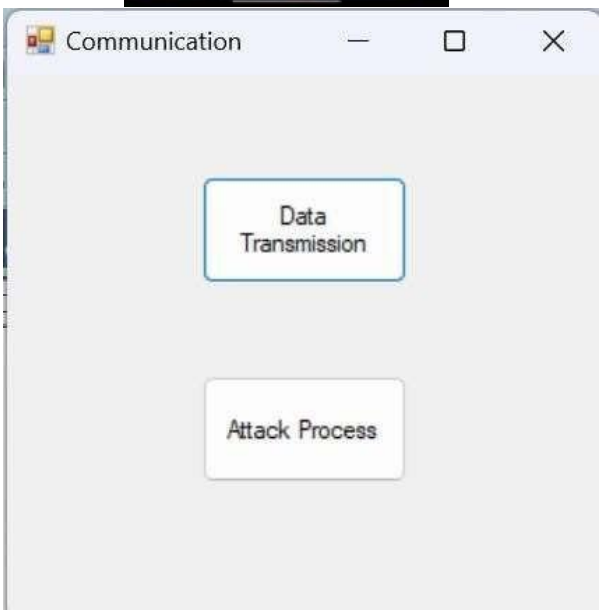


Figure 3.Detection Delay for existing and propose scheme

VI.RESULTS

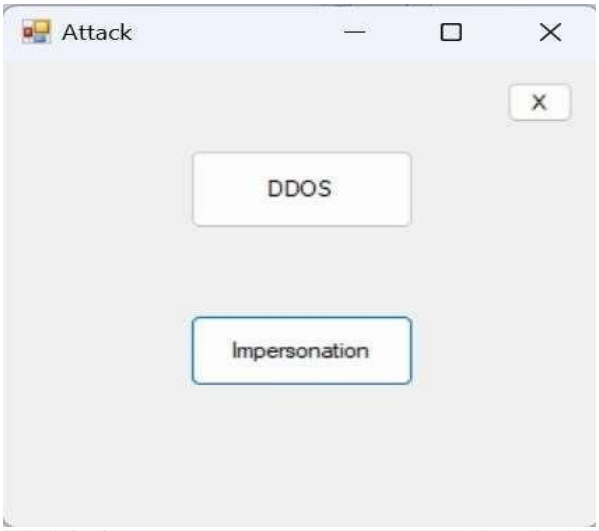
HOMEPAGE



COMMUNICATION TYPES

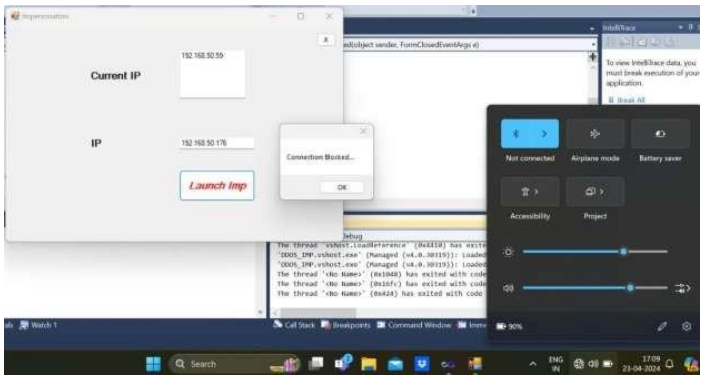
IDENTIFICATION OF DDoS ATTACK

LAUNCHING OF IMPERSONATION



LAUNCHING OF DDOS ATTACK

MITIGATING IMPERSONATION ATTACK



VI.CONCLUSION AND FUTURE SCOPE

The system has strong capabilities in protecting user data and privacy through the development and integration of modules for open Wi-Fi generation, device connection, attack simulation, and detection/mitigation.

The solution improves the security posture of public Wi-Fi settings by recognizing possible risks and gaps in current systems and implementing efficient tactics for threat detection and mitigation.

In future, these defences will need to be continuously improved upon and adjusted in order to keep people safe from emerging cyberthreats in an ever-changing digital environment.

REFRENCES

[1] Agyemang, J.O., Kponyo, J.J., Klogo, G.S. and Boateng, J.O., 2020. Lightweight rogue access point detection algorithm for WiFi-enabled Internet of Things (IoT) devices. Internet of Things, 11, p.100200.

[2] Jaysankar, R., Mohan, V.S. and Sankaran, S., 2023. Machine Learning–Based Approach for Detecting Beacon Forgeries in Wi-Fi Networks. In Artificial Intelligence and Deep Learning for Computer Network (pp. 13-33). Chapman and Hall/CRC.

[3] DA Arisandi, D., Nazrul Muhaimin Ahmad, N.M., Subarmaniam, A. and L Kannan, S.K., 2021. The rogue access point identification: a model and classification review. The Indonesian Journal of Electrical Engineering and Computer Science, 23(3), pp.1527-1537.

[4] Asaduzzaman, M., Majib, M.S. and Rahman, M.M., 2020, June. Wi-fi frame classification and feature selection analysis in detecting evil twin attack. In 2020 IEEE Region 10 Symposium (TENSYMP) (pp. 1704-1707). IEEE.

[5] Yang, Z., Lu, Q., Zhang, H., Chen, F. and Xian, H., 2023. Eliminating Rogue Access Point Attacks in IoT: A Deep Learning Approach With Physical-Layer Feature Purification and Device Identification. IEEE Internet of Things Journal.

[6] Ahadi, S.A.A., 2020, December. Overview on public wi-fi security threat evil twin attack detection. In 2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation (ICATMRI) (pp. 1-6). IEEE.

[7] Yan, D., Yan, Y., Yang, P., Song, W.Z., Li, X.Y. and Liu, P., 2022. Real-time identification of rogue WiFi connections in the wild. IEEE Internet of Things Journal, 10(7), pp.6042- 6058.

[8] Uszko, K., Kasprzyk, M., Natkaniec, M. and Chołda, P., 2023. Rule-based system with machine learning support for detecting anomalies in 5G WLANs. Electronics, 12(11), p.2355.

[9] Swetha, A. and Shailaja, K., 2020. An Effective Approach for Security Attacks Based on Machine Learning Algorithms. In Advances in Computational Intelligence and Informatics: Proceedings of ICACII 2019 (pp. 293-299). Springer Singapore.

[10] Ahadi, S.A.A., Baray, E., Rakesh, N. and Varshney, S., 2022, March. Public Wi-Fi security threat evil twin attack detection based on signal variant and hop count. In AIP Conference Proceedings (Vol. 2424, No. 1). AIP Publishing.

[11] Satam, P. and Hariri, S., 2020. WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol. IEEE Transactions on Network and Service Management, 18(1), pp.1077-1091.

[12] Srinivas, B., Puri, B., Vamshikrishna, Y. and Triveni, B., UNAUTHORIZED ACCESS POINT DETECTION USING MACHINE LEARNING ALGORITHMS FOR INFORMATION PROTECTION.

[13] Rofoo, F.F.H., Galety, M.G., Arulkumar, N. and Maaroof, R., 2022. DPETAs: Detection and Prevention of Evil Twin Attacks on Wi-Fi Networks. In Sustainable Advanced Computing: Select Proceedings of ICSAC 2021 (pp. 559-568). Singapore: Springer Singapore.

[14] Banakh, R., Piskozub, A. and Opirskyy, I., 2023. DEVISING A METHOD FOR DETECTING “EVIL TWIN” ATTACKS ON IEEE 802.11 NETWORKS (WI-FI) WITH KNN CLASSIFICATION MODEL. Eastern-European Journal of Enterprise Technologies, 123(9).

[15] Elhigazi Abdallah, A., Hamdan, M., Abd Razak, S., A Ghalib, F., Hamzah, M., Khan, S., Ahmed Babikir Ali, S., HH Khairi, M. and Salih, S., 2022. Resource Exhaustion Attack Detection Scheme for WLAN Using Artificial Neural Network. Computers, Materials &Continua,74(3)