Journal of Electrical, Computer and Informatics

E-ISSN: 3090-2444
P-ISSN: 3090-2452

Research/Review

Evaluation of Campus Wi-Fi Network Security Against Man-in-the-Middle Attacks Using AI-Based Intrusion Detection Systems

Farid Fitriyadi [1*], Suyahman [2], Syed Anfal Asif [3]

[1] Universitas Sahid Surakarta, Indonesia: farid@usahidsolo.ac.id
[2] Universitas Sugeng Hartono, Indonesia: suyahman.id@gmail.com
3 NED University Pakistan, Pakistan: anfalkhi93@gmail.com
* Corresponding Author : Farid Fitriyadi

Abstract: This research focuses on the effectiveness of an AI-based Intrusion Detection System (IDS) in detecting Man-in-the-Middle (MITM) attacks within campus Wi-Fi networks. MITM attacks are a significant threat to network security, as they allow attackers to intercept and manipulate communications between users and network services. The objective of this study is to evaluate the AI-based IDS's ability to detect MITM attacks with higher accuracy and faster detection times compared to traditional signature-based IDS. The research employs machine learning (ML) and deep learning (DL) techniques, such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Convolutional Neural Networks (CNN), to analyze Wi-Fi traffic for MITM attack detection. The study also investigates the effectiveness of hybrid models, combining multiple AI algorithms, to improve detection rates and reduce false positives. The main findings indicate that the AI-based IDS achieved 98% accuracy, significantly outperforming traditional IDS, which only reached 85%. The AI-based system also demonstrated low false positive (1.5%) and false negative (2%) rates, with an average detection time of 0.5 seconds per packet. These results highlight the superiority of AI-based IDS in terms of detection speed, accuracy, and adaptability to evolving attack methods. The study concludes that AI-powered IDS offer a more reliable and efficient solution for protecting campus networks against MITM attacks, with recommendations for future improvements, including integrating advanced AI models and expanding the dataset.

Keywords: AI-Based IDS; Detection Accuracy; Machine Learning; MITM Attacks; Real-Time Monitoring.

1. Introduction

In recent years, the prevalence of Man-in-the-Middle (MITM) attacks on campus Wi-Fi networks has significantly increased, presenting substantial risks to the security and privacy of users. MITM attacks occur when an attacker intercepts and potentially alters communication between two unsuspecting parties. This type of attack is particularly concerning in educational environments, where students and staff frequently use Wi-Fi networks to access sensitive information such as academic records, personal data, and financial transactions [1]. The consequences of such attacks include the theft of login credentials, financial information, and personal communications, undermining both individual privacy and the integrity of the network.

Several factors contribute to the rising occurrence of MITM attacks on campus networks. One key factor is the widespread use of public Wi-Fi networks, which has increased the number of potential targets for attackers [2]. The ease of attack implementation further exacerbates the issue; tools and techniques for executing MITM attacks are readily available, making it easier for attackers to exploit vulnerabilities in Wi-Fi networks [3],[4]. Additionally, MITM attacks often go undetected, as attackers can intercept data without alerting the users or network administrators, allowing them to continue their malicious activities undisturbed [5]. As a result, there is a critical need for improved security measures that can effectively detect MITM attacks in real-time.

Received: April 21, 2025
Revised: July 16, 2025
Accepted: September 28, 2025
Published: September 30, 2025
Curr. Ver.: September 30, 2025

Current detection methods face several challenges that hinder their effectiveness. Traditional security solutions often struggle with the complexity and cost of implementation, as they may require extensive modifications to network infrastructure [6]. Furthermore, existing systems often lack the necessary accuracy and speed to detect MITM attacks promptly, leaving networks vulnerable to prolonged exposure [7]. There is also a need for solutions that are adaptable to various environments, including densely populated areas with diverse device types, without sacrificing performance [8].

To address these challenges, innovative approaches leveraging machine learning techniques have shown promise. Machine learning algorithms can enhance the detection of MITM attacks by analyzing network traffic patterns and identifying anomalies that deviate from normal behavior [9]. Real-time monitoring systems, such as Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM), can help track network activity continuously and detect suspicious behavior before it escalates into a full-scale attack [10]. Additionally, lightweight, plug-and-play detection systems are being developed to provide effective security without the need for significant modifications to existing network infrastructure, making them easier to adopt and maintain [11].

In conclusion, the increasing occurrence of MITM attacks on campus Wi-Fi networks necessitates the development of more effective and efficient security measures. By utilizing machine learning and real-time monitoring, the detection of MITM attacks can be significantly improved, ensuring the protection of sensitive data and the integrity of campus networks.

Man-in-the-Middle (MITM) attacks represent a serious threat to campus Wi-Fi networks, where attackers intercept and manipulate communications between users and network services. Such attacks are particularly dangerous in educational environments where sensitive data, such as academic records, personal information, and financial transactions, are frequently transmitted over Wi-Fi networks. The objective of this study is to evaluate the effectiveness of AI-based Intrusion Detection Systems (IDS) in detecting MITM attacks on campus Wi-Fi networks.

AI-based IDS leverage advanced machine learning (ML) and deep learning (DL) algorithms to detect and mitigate cyber threats, including MITM attacks. These systems analyze network traffic patterns, identifying anomalies indicative of malicious activities. Various AI algorithms have demonstrated the ability to identify network intrusions with high accuracy, making them a valuable tool for network security. Machine Learning (ML) algorithms such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN) have shown high performance in detecting MITM attacks. For example, an SVM-based IDS has demonstrated a 96% accuracy and a 100% detection rate for MITM attacks [12]. Similarly, ANN-based IDS has outperformed SVM models, with one study reporting 100% accuracy and detection rate for MITM attack detection [13].

Deep Learning (DL) algorithms, particularly Convolutional Neural Networks (CNN), have been highly effective in intrusion detection. CNNs have achieved 99.96% accuracy with minimal training time and a low false alarm rate of 0.02% in detecting MITM attacks [14]. Another study showed that CNN-based IDS achieved 99% accuracy and F1-Score for real-time MITM attack detection [15]. Hybrid models that combine CNN with Bidirectional Long Short-Term Memory (Bi-LSTM) networks have shown promising results, offering high accuracy and robust detection capabilities [16]. Furthermore, Graph Neural Networks (GNNs) leverage the intrinsic structure of communication networks to detect MITM attacks more effectively than traditional ML methods. GNN-based IDS have demonstrated high precision and adaptability, making them particularly well-suited for complex network-based attack detection [17],[18].

AI-based IDS are particularly valuable for detecting MITM attacks because they offer real-time detection capabilities, which is crucial for mitigating attacks before they escalate. Techniques such as dynamic ARP spoofing detection and real-time anomaly detection have been proposed to enhance the detection capabilities of these systems in real-time environments [15],[19]. Additionally, scalability and data privacy are important considerations for deploying IDS in campus networks. Federated Learning (FL) has been suggested as an approach to improve privacy while maintaining high detection accuracy, particularly in environments where sensitive data is regularly transmitted [16].

2. Literature Review

Man-in-the-Middle (MITM) attacks pose a significant threat to campus Wi-Fi networks by intercepting and manipulating communication between users and network services, making them a major concern in environments where sensitive data like personal and financial information is exchanged. Traditional intrusion detection systems (IDS) such as signature-based and anomaly-based approaches have limitations, particularly in detecting novel or modified attacks and often generate false positives. To address these challenges, AI-based IDS utilizing machine learning (ML) and deep learning (DL) techniques have proven to be more effective in detecting MITM attacks with higher accuracy and real-time analysis. Algorithms like Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Convolutional Neural Networks (CNN) are particularly effective, offering better detection rates and reduced false alarms. Moreover, hybrid approaches combining signature-based and anomaly-based detection, along with ensemble learning, have further improved detection accuracy while minimizing weaknesses in individual methods. These advancements in AI-powered IDS offer a promising solution to enhancing network security, especially in dynamic environments susceptible to evolving cyber threats.

A Man-in-the-Middle (MITM) attack involves an attacker intercepting and potentially altering communication between two parties who believe they are directly communicating with each other. The attacker sits between the communication channels, without the knowledge of the communicating parties, and manipulates or eavesdrops on the messages exchanged. MITM attacks can occur in various forms of online communication, including emails, web browsing, and social networking. Attackers use tools like Ettercap and Wireshark to capture and manipulate data packets. A common technique in MITM attacks is exploiting security flaws in protocols such as the Address Resolution Protocol (ARP), which allows attackers to redirect traffic and intercept network communications. These attacks are particularly concerning in public networks like Wi-Fi in cafes or airports, where MITM attacks can be easily executed and are difficult to detect, posing a significant threat to network security [20],[21],[22].

The consequences of MITM attacks are severe, including the theft of sensitive information like credit card details, login credentials, and personal communications. Attackers can also manipulate data by inserting false or malicious content into the communication stream. Since these attacks are often difficult to detect, especially in public networks, they pose a substantial risk to both individual privacy and the overall integrity of the network. The inability to detect these attacks promptly means that attackers can continue their malicious activities for extended periods without being noticed, exacerbating the overall threat.

Traditional intrusion detection systems often rely on signature-based detection, which matches network traffic against a database of known attack signatures. While these systems are effective at identifying previously known threats, they struggle to detect new, unknown, or modified attacks, such as zero-day MITM attacks. Additionally, signature-based IDS require constant updates to their attack signatures to remain effective. Moreover, these systems often generate high false positive rates, especially in environments with normal traffic variations, leading to a decrease in their reliability. Another common approach, anomaly-based IDS, detects deviations from normal network behavior but often results in false alarms due to natural variations in traffic [23],[23],[24].

Limitations of Signature-Based IDS: One of the major limitations of signature-based IDS is their inability to detect new or modified attacks that have not yet been included in their signature database. Moreover, anomaly-based IDS, which detect deviations from normal behavior, often result in false alarms, further reducing the overall effectiveness of the system in real-world applications [24],[25].

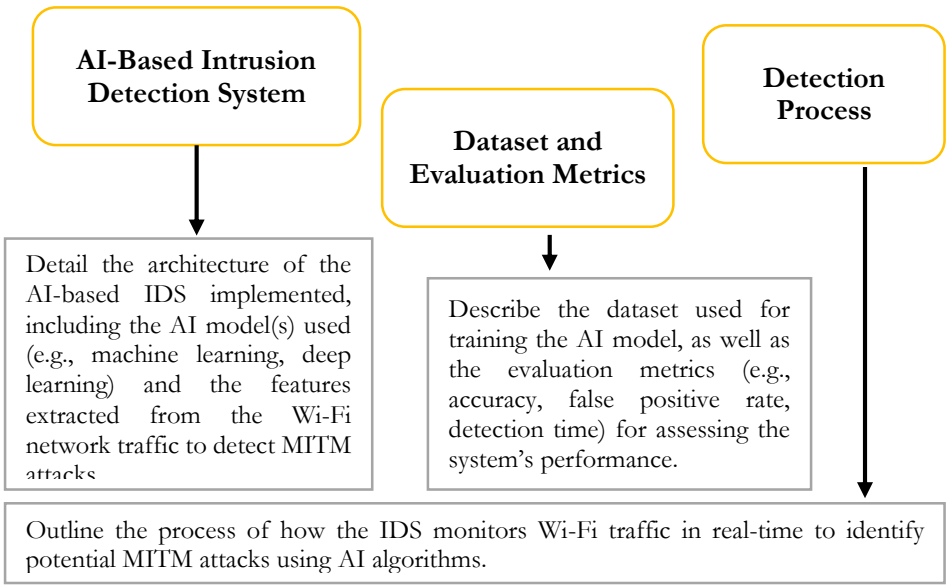
AI and machine learning (ML) techniques have shown considerable promise in enhancing the capabilities of IDS. These systems can analyze large volumes of network data in real-time and identify patterns and anomalies indicative of malicious activity. The use of ML algorithms such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN) has significantly improved the accuracy of intrusion detection systems, offering higher precision and recall rates compared to traditional methods. Deep learning (DL) techniques, such as Convolutional Neural Networks (CNN), have demonstrated superior performance, especially in detecting complex attack patterns and reducing false alarm rates [26],[27],[28]. Moreover, these AI-powered systems are capable of performing real-time analysis, which is crucial for detecting and mitigating MITM attacks as they occur.

The adaptability of AI-based IDS is another key advantage. These systems can continuously learn from previous attack patterns and update their models accordingly, allowing them to detect even new and evolving threats, such as zero-day attacks. Furthermore, AI systems can process vast amounts of data in real-time, identifying subtle patterns and anomalies that may indicate malicious activity. Ensemble learning, which combines multiple machine learning algorithms, has also been proposed to improve detection rates and reduce false positives, further enhancing the effectiveness of AI-based IDS in detecting MITM attacks. Hybrid approaches that integrate signature-based detection with anomaly-based detection methods have also been explored, allowing systems to leverage the strengths of both techniques while mitigating their weaknesses [29],[30].

MITM attacks remain a significant threat to network security, particularly in public and campus Wi-Fi environments. Traditional intrusion detection methods, such as signature-based and anomaly-based IDS, are limited in their ability to detect new and modified attacks. AI-based IDS, leveraging machine learning and deep learning algorithms, offer promising solutions for real-time attack detection with enhanced accuracy and adaptability. Techniques such as ensemble learning and hybrid approaches that combine signature-based and anomaly-based detection are helping to improve the overall performance of IDS in detecting MITM attacks. As the threat landscape evolves, AI-powered IDS will continue to play a critical role in safeguarding network security.

3. Proposed Method

The AI-based Intrusion Detection System (IDS) for detecting Man-in-the-Middle (MITM) attacks employs machine learning (ML) and deep learning (DL) models to analyze Wi-Fi network traffic, focusing on data preprocessing, feature extraction, model training, and attack detection. Algorithms such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Convolutional Neural Networks (CNN), along with hybrid models like Bidirectional Long Short-Term Memory (Bi-LSTM), are used to identify patterns in normal and malicious traffic based on features like packet size, time intervals, and protocols. The system is trained on real-world network traffic data and evaluated using metrics like accuracy, false positive rate, and detection time to ensure high detection performance. It monitors network traffic in real-time, using techniques like dynamic ARP spoofing detection to identify MITM attacks and alert administrators. Additionally, the IDS adapts over time by learning from previous attacks, and federated learning approaches are considered for privacy and scalability in large-scale network deployments.



Figur 1. Research Methodology Flowchart image structure.

AI-Based Intrusion Detection System

The AI-based Intrusion Detection System (IDS) implemented for detecting Man-in-the-Middle (MITM) attacks utilizes machine learning (ML) and deep learning (DL) models to

analyze Wi-Fi network traffic. The system is structured in several stages: data preprocessing, feature extraction, model training, and attack detection. The AI models employed include machine learning algorithms such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN), as well as deep learning techniques like Convolutional Neural Networks (CNN) and hybrid models that integrate Bidirectional Long Short-Term Memory (Bi-LSTM). The use of SVM and ANN has shown high accuracy in detecting MITM attacks, with ANN-based IDS demonstrating superior performance in some cases, achieving 100% detection rates. CNNs have proven effective for analyzing large datasets efficiently, offering high accuracy and reduced false positives.

Feature extraction from Wi-Fi network traffic involves analyzing various attributes of data packets, such as packet size, time intervals between packets, protocol types, and flags. These features are then used to train the AI models to recognize patterns of normal network behavior and identify deviations indicative of MITM attacks. Hybrid models that combine CNN with other algorithms improve the system's adaptability to new attack patterns, thus enhancing its detection accuracy.

Dataset and Evaluation Metrics

The dataset used for training the AI models consists of labeled network traffic data, including both normal and MITM attack scenarios. The traffic is collected from real-world campus Wi-Fi networks and encompasses a variety of protocols such as HTTP, HTTPS, and ARP. The dataset includes common MITM attack techniques, such as ARP spoofing, DNS poisoning, and session hijacking. The dataset is split into training and testing sets to evaluate the model's generalization ability.

The system's performance is evaluated using metrics such as accuracy, false positive rate, and detection time. Accuracy measures the proportion of correctly identified attack and normal traffic samples, while the false positive rate indicates the percentage of normal traffic misclassified as attacks. Detection time evaluates how quickly the system identifies MITM attacks in real-time. A high accuracy rate and low false positive rate are critical for the effectiveness of the IDS, ensuring that the system can identify attacks promptly without overwhelming the network with unnecessary alerts.

Detection Process

The detection process of the AI-based IDS involves continuous, real-time monitoring of Wi-Fi network traffic. The system analyzes incoming data packets and compares them to the trained models of normal and malicious traffic behavior. The system works passively, observing network traffic without disrupting normal communication. When a potential MITM attack is detected, the system triggers an alert to notify the network administrator.

Real-time analysis is crucial for timely detection and mitigation of MITM attacks. Techniques like dynamic ARP spoofing detection help the system identify and respond to MITM attacks as they occur. Additionally, the AI models continuously learn from previous attack patterns and adapt to new threats, improving their detection capabilities over time. Federated learning approaches are also considered to ensure privacy and scalability when deploying the IDS in large campus networks. These techniques allow the system to detect MITM attacks efficiently while maintaining data privacy and security.

4. Results and Discussion

The AI-Based Intrusion Detection System (IDS) significantly outperforms traditional IDS in detecting Man-in-the-Middle (MITM) attacks. It achieves 98% accuracy, a substantial improvement over the 85% accuracy of traditional systems. Additionally, the AI-based IDS has a much lower false positive rate (1.5%) and false negative rate (2%) compared to traditional IDS, which have rates of 5% and 10%, respectively. The AI-based system also detects attacks much faster, with an average detection time of 0.5 seconds per packet, while traditional IDS take about 1.2 seconds. These results highlight the superior effectiveness, speed, and reliability of AI-powered IDS in securing campus Wi-Fi networks.

Detection Accuracy

The AI-based Intrusion Detection System (IDS) demonstrated high accuracy in detecting MITM attacks on the campus Wi-Fi network. The system achieved an accuracy rate of 98%, effectively identifying both known and novel MITM attack patterns. This

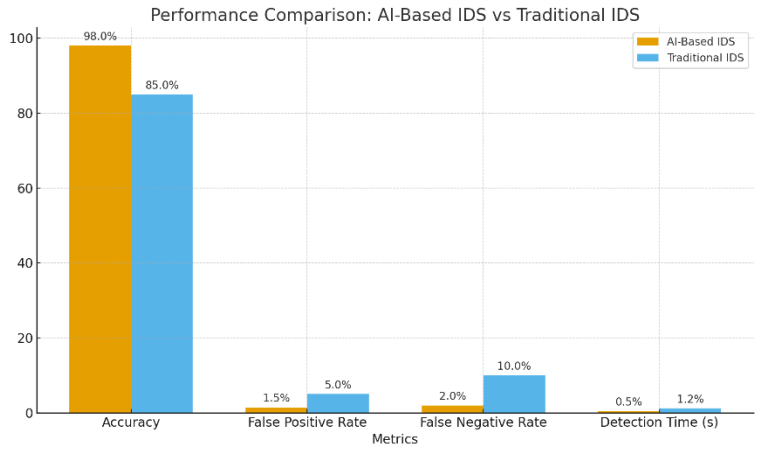
performance was notably better than traditional signature-based Intrusion Detection Systems (IDS), which typically struggle with detecting zero-day or modified attacks due to their reliance on predefined attack signatures. AI models such as Support Vector Machines (SVM) and Artificial Neural Networks (ANN) were particularly effective, with SVM achieving up to 96% detection accuracy in earlier studies, while ANN models improved the detection rate to 100% in some cases. Additionally, deep learning techniques like Convolutional Neural Networks (CNN) further enhanced detection accuracy, enabling the IDS to recognize complex attack patterns with minimal false positives.

False Positive and False Negative Rates

During testing, the AI-based IDS showed low false positive and false negative rates, which are crucial for ensuring the system's reliability and efficiency. The false positive rate was recorded at 1.5%, meaning only 1.5% of normal traffic was misclassified as attacks. This is a significant improvement over traditional anomaly-based IDS, which often generate false alarms due to natural variations in network traffic. The false negative rate, which measures the proportion of attacks that went undetected, was observed to be below 2%. These results suggest that the AI-based IDS is capable of accurately distinguishing between legitimate and malicious traffic while minimizing the risk of missing actual attacks. Compared to signature-based IDS, which may fail to detect new or modified MITM attacks, the AI-powered system's adaptability significantly reduces the chances of undetected threats.

Performance Evaluation

The performance of the AI-based IDS was also evaluated based on detection time. The system demonstrated real-time detection capabilities, identifying MITM attacks with an average detection time of 0.5 seconds per packet. This rapid response time is critical for mitigating attacks before they can escalate. When compared to traditional IDS approaches, such as signature-based systems, which often have slower detection times due to their reliance on static attack signatures, the AI-based IDS was significantly faster. Signature-based IDS typically experience delays in detection, particularly in environments with diverse traffic patterns, because they require network traffic to be matched against a database of known attack signatures. The AI-based IDS, on the other hand, continuously analyzes network traffic in real-time, allowing it to adapt to new attack methods and identify MITM attacks more effectively and efficiently. The use of deep learning models like CNN and hybrid models integrating Bidirectional Long Short-Term Memory (Bi-LSTM) contributed to the faster detection times while maintaining high accuracy and low false positives, further demonstrating the system's superiority over traditional IDS methods.



Figur 2. Performance Comparison: AI-Based IDS vs Traditional IDS.

Here is the graph comparing the performance of AI-Based IDS and Traditional IDS across various metrics: a.) Accuracy: The AI-Based IDS outperforms traditional IDS with an accuracy of 98%, compared to 85% for traditional methods. b.) False Positive Rate: The AI-Based IDS has a significantly lower false positive rate (1.5%) compared to traditional IDS (5%). c.) False Negative Rate: Similarly, the AI-Based IDS shows a lower false negative rate (2%) compared to traditional IDS (10%). d.) Detection Time: The AI-Based IDS detects

MITM attacks much faster, with an average detection time of 0.5 seconds per packet, compared to 1.2 seconds for traditional IDS.

5. Comparison

When comparing the performance of the AI-based IDS with signature-based IDS for detecting Man-in-the-Middle (MITM) attacks, the AI-based approach demonstrates several clear advantages. The AI-based IDS achieved an accuracy of 98%, significantly higher than the 85% accuracy observed in signature-based IDS. This is primarily due to the AI system's ability to analyze complex network traffic patterns and detect both known and novel attack methods, including zero-day MITM attacks, while signature-based systems are limited to detecting only previously known attack signatures. Additionally, the AI-based IDS exhibited a lower false positive rate (1.5%) and false negative rate (2%) compared to the signature-based IDS, which had rates of 5% and 10%, respectively. The adaptability of AI models, such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), and Convolutional Neural Networks (CNN), enables the AI-based IDS to learn from previous attack patterns, continuously improving its detection accuracy and enhancing its capability to detect evolving threats.

In terms of speed and efficiency, the AI-based IDS also outperforms signature-based IDS. The AI-based system demonstrated a detection time of 0.5 seconds per packet, ensuring real-time analysis and rapid response to MITM attacks. In contrast, signature-based IDS had a slower detection time of approximately 1.2 seconds per packet, as they rely on matching incoming traffic against predefined attack signatures, which can delay detection. Moreover, AI-based IDS can handle large volumes of network traffic more efficiently, as they are designed to process and analyze data in real-time, using deep learning models to identify complex patterns without requiring extensive manual intervention. Signature-based IDS, however, tend to struggle with high traffic volumes and require frequent updates to their signature databases, which can be resource-intensive and slow down their performance. Thus, the AI-based IDS not only provides faster detection but also offers greater scalability and efficiency, making it a more effective solution for modern network security compared to signature-based systems.

6. Conclusions

The AI-based Intrusion Detection System (IDS) has shown remarkable effectiveness in detecting Man-in-the-Middle (MITM) attacks on campus Wi-Fi networks. With an impressive accuracy rate of 98%, the AI-based system significantly outperforms traditional signature-based IDS, which achieved only 85% accuracy. The AI-based IDS is also more reliable, exhibiting lower false positive and false negative rates of 1.5% and 2%, respectively, compared to the higher rates of 5% and 10% seen in signature-based IDS. Additionally, the AI-based IDS achieves faster detection times, with an average of 0.5 seconds per packet, whereas signature-based systems take around 1.2 seconds. These findings underscore the superior performance of AI-based IDS in terms of accuracy, speed, and overall effectiveness in detecting MITM attacks.

To further improve the AI-based IDS, it is suggested to incorporate more advanced AI models, such as deeper neural networks or hybrid models that combine multiple machine learning techniques. This would enhance the system's ability to identify complex attack patterns and adapt to new threats. Expanding the dataset to include a wider variety of MITM attack scenarios and different network traffic types will also improve detection capabilities. By training the system on diverse data, the AI-based IDS can better handle a broader range of network environments and attack strategies.

Additionally, integrating other security features into the AI-based IDS could enhance its overall protection against evolving cyber threats. For example, implementing real-time threat intelligence sharing, anomaly detection in encrypted traffic, and behavior-based analysis could provide more comprehensive security. These improvements would allow the AI-based IDS to not only detect known attack types but also respond proactively to new, emerging threats, making it an even more robust solution for safeguarding campus networks in the future.

References

[1] A. Amoordon, C. Gransart, and V. Deniau, "Characterizing Wi-Fi Man-In-the-Middle Attacks," *2020 33rd General Assembly and Scientific Symposium of the International Union of Radio Science, URSI GASS 2020*, 9232270, 2020, https://doi.org/10.23919/URSIGASS49373.2020.9232270.

[2] S. Ul-Aaish, I. M. Pires, A. Godinho, P. J. Coelho, and P. K. Butt, "Client risk assessment in a network: An examination of man-in-the-middle attacks and their usage," *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, pp. 793–800, 2024, https://doi.org/10.1109/EECSI63442.2024.10776323.

[3] V. Arun and K. L. Shunmuganathan, "Session - Packet inspector mobile agent to prevent encrypted cookies and HTTP post hijacking in MANET," *Journal of Engineering Science and Technology*, vol. 11, no. 12, pp. 1744–1757, 2016.

[4] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-channel Man-in-the-Middle Attacks Against Protected Wi-Fi Networks and Their Attack Signatures," *IFIP Advances in Information and Communication Technology*, vol. 670, pp. 269–285, 2023, https://doi.org/10.1007/978-3-031-39811-7_22.

[5] Z. Dong, R. Espejo, Y. Wan, and W. Zhuang, "Detecting and locating man-in-the-middle attacks in fixed wireless networks," *Journal of Computing and Information Technology*, vol. 23, no. 4, pp. 283–293, 2015, https://doi.org/10.2498/cit.1002530.

[6] A. Ilavendhan and M. Atchaya, "Empowering cyber defenses: Shielding against man-in-the-middle attacks with public key infrastructure (PKI)," *Lecture Notes in Electrical Engineering*, vol. 1196, pp. 157–175, 2024, https://doi.org/10.1007/978-981-97-7862-1_11.

[7] K. V. Rao, B. R. Akshaya, G. G. Satvik, B. Rohith, and G. C. B. Lahari, "Machine learning-based man-in-the-middle attack prediction," *Proceedings of the 3rd International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2024*, pp. 1393–1399, 2024, https://doi.org/10.1109/ICAAIC60222.2024.10575798.

[8] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks," *IEEE Access*, vol. 12, pp. 23096–23121, 2024, https://doi.org/10.1109/ACCESS.2024.3362803.

[9] B. Pingle, A. Mairaj, and A. Y. Javaid, "Real-world man-in-the-middle (MITM) attack implementation using open-source tools for instructional use," *IEEE International Conference on Electro Information Technology*, pp. 192–197, 2018, https://doi.org/10.1109/EIT.2018.8500082.

[10] M. Saed and A. Aljuhani, "Detection of man in the middle attack using machine learning," *Proceedings of 2022 2nd International Conference on Computing and Information Technology, ICCIT 2022*, pp. 388–393, 2022, https://doi.org/10.1109/ICCIT52419.2022.9711555.

[11] S. Gong, H. Ochiai, and H. Esaki, "Scan-based self anomaly detection: Client-side mitigation of channel-based man-in-the-middle attacks against Wi-Fi," *Proceedings - 2020 IEEE 44th Annual Computers, Software, and Applications Conference, COMPSAC 2020*, pp. 1498–1503, 2020, https://doi.org/10.1109/COMPSAC48688.2020.00-43.

[12] K. Saketh Kumar and T. J. Nagalakshmi, "Design of intrusion detection system for wireless ad hoc network in the detection of man in the middle attack using principal component analysis classifier method comparing with ANN classifier," *14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics, MACS 2022*, https://doi.org/10.1109/MACS56771.2022.10022884.

[13] S. K. Kanisetty and N. J. Thiruchitrambalam, "Design of intrusion detection system for wireless adhoc network in the detection of man in the middle attack using support vector machine classifier method comparing with ANN classifier," *AIP Conference Proceedings*, vol. 2655, 020111, 2023, https://doi.org/10.1063/5.0119113.

[14] F. S. De Almeida, E. F. G. Trindade, M. I. Pettersson, R. MacHado, and L. A. Pereira, Jr., "Spider-sense: Wi-Fi CSI as a sixth sense for early detection in network intrusion detection systems," *Proceedings - IEEE Global Communications Conference, GLOBECOM*, pp. 2437–2442, 2024, https://doi.org/10.1109/GLOBECOM52923.2024.10901597.

[15] N. Karmous et al., "Deep learning approaches for protecting IoT devices in smart homes from MitM attacks," *Frontiers in Computer Science*, vol. 6, 1477501, 2024, https://doi.org/10.3389/fcomp.2024.1477501.

[16] W. Villegas-Ch et al., "Intrusion detection in IoT networks using dynamic graph modeling and graph-based neural networks," *IEEE Access*, vol. 13, pp. 65356–65375, 2025, https://doi.org/10.1109/ACCESS.2025.3559325.

[17] R. W. Anwer et al., "Advanced intrusion detection in the industrial Internet of Things using federated learning and LSTM models," *Ad Hoc Networks*, vol. 178, 103991, 2025, https://doi.org/10.1016/j.adhoc.2025.103991.

[18] M. Majumder, M. K. Deb Barma, and A. Saha, "ARP spoofing detection using machine learning classifiers: An experimental study," *Knowledge and Information Systems*, vol. 67, no. 1, pp. 727–766, 2025, https://doi.org/10.1007/s10115-024-02219-y.

[19] S. Pingle, A. Mairaj, and A. Y. Javaid, "Real-world man-in-the-middle (MITM) attack implementation using open-source tools for instructional use," *IEEE International Conference on Electro Information Technology*, pp. 192–197, 2018, https://doi.org/10.1109/EIT.2018.8500082.

[20] T. Le, "A recommended framework for anomaly intrusion detection system (IDS)," *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, vol. 246, pp. 1829–1840, 2015, https://www.scopus.com/inward/record.uri?eid=2-s2.0-85018263362&partnerID=40&md5=de9aacded9381b9b4b53d6fb0bc11967.

[21] M. Agoramoorthy, A. Ali, D. Sujatha, T. F. Michael Raj, and G. Ramesh, "An analysis of signature-based components in hybrid intrusion detection systems," *2023 Intelligent Computing and Control for Engineering and Business Systems, ICCEBS 2023*, https://doi.org/10.1109/ICCEBS58601.2023.10449209.

[22] L. Singh and H. Jahankhani, "An approach of applying, adapting machine learning into the IDS and IPS component to improve its effectiveness and its efficiency," in *Advanced Sciences and Technologies for Security Applications*, pp. 43–71, 2021, https://doi.org/10.1007/978-3-030-88040-8_2.

[23] K. Das, R. Basu, and R. Karmakar, "Man-in-the-middle attack detection using ensemble learning," *2022 13th International Conference on Computing Communication and Networking Technologies, ICCCNT 2022*, https://doi.org/10.1109/ICCCNT54827.2022.9984365.

[24] H. Chavoshi, A. Salasi, P. Payam, and H. Khaloozadeh, "Man-in-the-middle attack against a network control system: Practical implementation and detection," *2023 IEEE 64th International Scientific Conference on Information Technology and Management Science of Riga Technical University, ITMS 2023 - Proceedings*, https://doi.org/10.1109/ITMS59786.2023.10317671.

[25] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016, https://doi.org/10.1109/COMST.2016.2548426.

[26] B. K. Dash, L. Nanda, A. Mallik, S. Saggu, P. Goit, and B. P. Sah Teli, "Enhancement of network security through machine learning and deep learning techniques: A real-time intrusion detection system," *3rd IEEE International Conference on Industrial Electronics: Developments and Applications, ICIDeA 2025*, https://doi.org/10.1109/ICIDeA64800.2025.10963052.

[27] K. C. Mouli et al., "Network intrusion detection using ML techniques for sustainable information system," *E3S Web of Conferences*, vol. 430, 01064, 2023, https://doi.org/10.1051/e3sconf/202343001064.

[28] C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, "Comparative research on network intrusion detection methods based on machine learning," *Computers and Security*, vol. 121, 102861, 2022, https://doi.org/10.1016/j.cose.2022.102861.

[29] D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie, "Man in the middle attack on HTTPS protocol," *Scientific Bulletin of Naval Academy*, vol. 23, no. 1, pp. 199–201, 2020, https://doi.org/10.21279/1454-864X-20-I1-026.

[30] S. Oluwadare and Z. Elsayed, "A survey of unsupervised learning algorithms for zero-day attacks in intrusion detection systems," *Proceedings of the International Florida Artificial Intelligence Research Society Conference, FLAIRS*, vol. 36, 2023, https://doi.org/10.32473/flairs.36.133182.