JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Machine Learning Techniques for Detecting ARP Spoofing Attack: A Review

Buli Fakada*, Dr.Gaurav Gupta,**
*M.Tech Scholar, Department of Computer Science and Engineering
Punjabi University, Patiala
**Assistant Professor
Department of Computer Science and Engineering
Punjabi University, Patiala
gaurav.shakti@gmail.com

Abstract: Address Resolution Protocol (ARP) spoofing poses a critical threat to network security, enabling Man-in-the-Middle attacks that allow malicious actors to intercept and manipulate communication between devices. Traditional security mechanisms often prove inadequate against these sophisticated attacks, necessitating the exploration of advanced detection methods.

This review differentiates packet spoofing techniques and evaluates how different machine learning Machine Learning models can detect anomalous ARP traffic patterns in order to determine how effective ML techniques are at detecting and preventing ARP spoofing-based man in the middle attacks. In this review thoroughly investigates a variety of machine learning-based techniques, such as supervised (Decision Trees, (KNN) K-Nearest Neighbors, Support Vector Machines, Random Forests, Logistic Regression), unsupervised, and deep learning (Convolutional Neural Networks, Long Short-Term Memory networks) models, evaluating their capacity to detect anomalous ARP traffic patterns.

The review evaluates the advantages and disadvantages of each approach, emphasizing the critical role of feature selection, dataset quality, and real-time processing capabilities. Furthermore, it addresses the challenges associated with deploying ML-based security solutions in practical network environments.

Keywords: Machine learning, ARP spoofing, MITM attacks, Network security, Intrusion detection, IoT

1. INTRODUCTION

Internet of Thing devices have made the world a connected place in various sectors, but their rise has made our networks vulnerable to many security attacks, one of which is the very famous Man-in-the- Middle type, especially exploiting vulnerabilities in the communication protocols. One of the standard methods of executing Man-in-the-Middle attacks is ARP spoofing. An attacker would associate their MAC address with the IP address of the virtual network website, transmitting spoofed ARP packets over the local network then removing the original data By such manipulation, communications between two parties can be intercepted, modified, or redirected without knowledge of either party Man-in-the-middle attacks are significant in compromising network security as an attacker can intercept and alter messages between two parties who think they are communicating securely [1].

The most commonly used ARP spoofing method that enables man in the middle attacks takes advantage of the vulnerabilities embedded in the ARP protocol for having no authentication mechanism [2].

This enables attackers to spoof ARP replies, mapping their MAC address to the IP address of a legitimate host, thereby redirecting network traffic through their own systems. The effects of successful ARP spoofing- based MITM attacks can be very devastating, from data interception and modification to denial-of-service and session hijacking [3]. Address Resolution Protocol spoofing attacks can have serious repercussions, such as data theft, sensitive information being accessed without authorization, and network services being interrupted [4]. To prevent ARP spoofing attacks, machine learning techniques appear to present a plausible solution in their detection. With large datasets and enhanced algorithms, such models would efficiently learn to discriminate between legitimate and unauthorized network packets. Given this proactive stance, the accurate detection of threats will be significantly improved, opening the doors for real-time human intervention in disease outbreaks, which will broadly strengthen the entire network system against such threats. With the ever-increasing adoption of these techniques, organizations will be much better positioned to protect their potential infrastructure from the evolving threat of cyber-attacks, allowing at least for improved security for their users and sensitive data [5].

Address Resolution Protocol spoofing, or ARP poisoning, is a specific type of authentication. The attacker will send forged ARP messages to assign their MAC address to the IP address of a device that is currently connected on the network. This allows the attacker to intercept, modify, or block traffic between devices. The purpose of this study were to differentiate the packet spoofing methods and saw how they can lead to a man-in-the- middle assault in one of the earlier articles in this series. But since hackers prefer this approach the most, we felt it was worthwhile to write an article specifically on it. As the name implies, the primary purpose of man-in-the-middle attack is to steal data and information that is important to business organizations. This attack is risky because it can be made viable by taking advantage of built-in flaws in the TCPIP protocol at different stages. It is technically a variation of packet sniffing and spoofing techniques, and if executed correctly, this attack can be totally undetectable to consumers, making. A man in the middle attack alters communication between two parties without their knowledge. Man-in-the-Middle attacks in cyber security are a severe threat to network integrity and confidentiality of data, particularly if they are ARP spoofing-based simple man in the middle attack model is shown in Figure 1 [6].

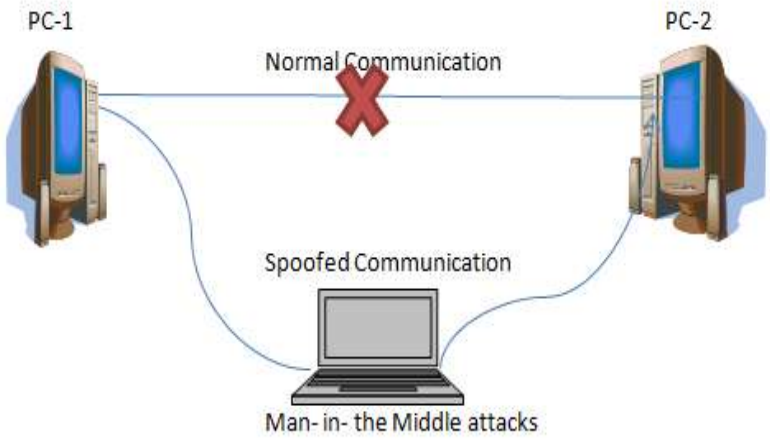

Figure 1: man-in-the-middle attack model.

These are two parties (e.g., computers, users, or servers) who want to communicate securely. In the normal situation, they ought to communicate directly represented by the blue arrow named Normal Communication. Man in the middle attack is the attacker (the computer in the middle) intercepts the communication between PC-1 and PC-2. Instead of communication directly between the two Targets, the attacker sets up two different connections: one between PC-1 and the attacker. This is shown by the red arrows labeled Spoofed Communication. The attacker can listen to confidential information passwords, banking information, and secret messages. The attacker is able to alter the messages before sending them. Targets have the impression that they are communicating directly, but they are communicating indirectly through the attacker. The attacker tricks the network into thinking their device is the legitimate gateway, redirecting traffic through them. Attackers send fake ARP messages to associate their MAC address with a legitimate IP address. It is used to intercept or modify network traffic that an attacker inserts himself into the communications tunnel.

2. ARP Spoofing attack Configuration

ARP spoofing is commonly used in the Ethernet. It is a fact that MAC determines the address in the Ethernet rather than in the IP. IP addresses (Internet Protocol addresses) are logical addresses used for routing packets across networks.MAC addresses (Media Access Control addresses) are physical addresses assigned to network interfaces for communication within a local network. If the Data Link Layer is unaware of the MAC address of the target IP, it will issue an ARP request to all hosts in the LAN. The only host that will reply with the target Internet Protocol is an Address Resolution Protocol reply from the source host in its MAC. In attempting to enhance the effectiveness of address conversion, there is always referred to as the ARP cache (i.e., the MAC entries in the memory of each host). The Address Resolution Protocol cache is a dynamic record to be used to record recent IP-MAC records. In the majority of operating systems, if an ARP responds, they will refresh their ARP caches, whether they sent an Address Resolution Protocol request or not. There are three stages to a complete man-in-the-middle assault that uses ARP spoofing model shown in Figure 2 [7].

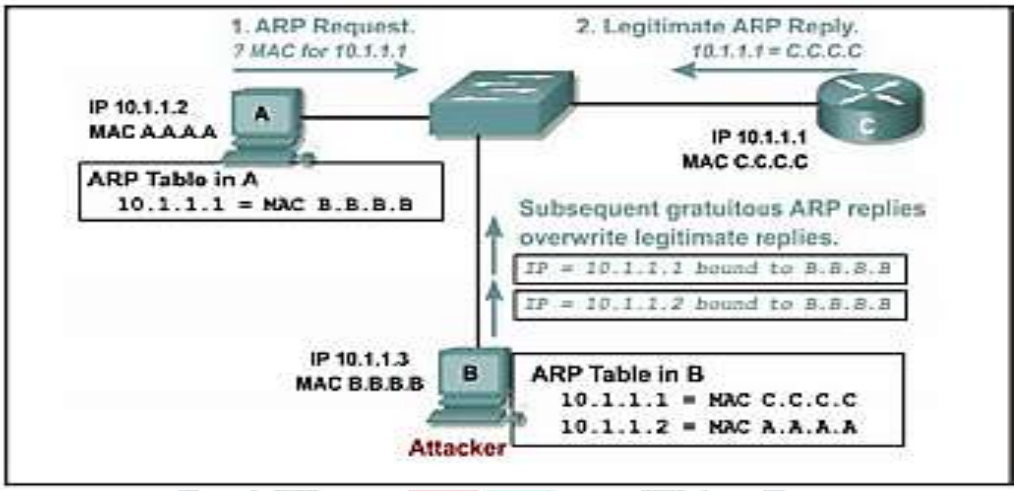

Figure 2: ARP spoofing attack configuration

3. ARP Spoofing: Nature and Threats

Address Resolution Protocol (ARP) is a stateless protocol that maps IP addresses to MAC addresses in a network. Its lack of authentication makes it susceptible to spoofing attacks, where malicious entities forge ARP replies to mislead a host about the MAC-IP mapping. This enables attackers to perform man-in-the-middle, session hijacking, and denial-of-service attacks (Gupta & Shukla, 2020).

4. Traditional Detection Approaches

Traditional detection approaches for ARP spoofing attacks typically rely on static rules, protocol-based monitoring, or predefined attack signatures. Methods such as **static ARP tables** involve manually assigning MAC-IP bindings to prevent spoofing, but these lack scalability in dynamic networks.

Signature-based Intrusion Detection Systems (IDS) compare network traffic to known attack patterns, yet they often fail against new or modified spoofing techniques.

Gratuitous ARP monitoring detects abnormal ARP broadcasts but is prone to false positives, as it struggles to distinguish between legitimate and malicious activity. While these conventional methods offer some protection, they are generally limited by rigidity, low adaptability, and poor performance in detecting evolving or stealthy ARP spoofing attacks.

5. Challenges in ARP Spoofing Detection

Machine Learning based there are several challenges associated with detecting ARP spoofing attacks:

- **Data Collection**: Obtaining a high-quality dataset that accurately reflects both normal and spoofed ARP traffic is non-trivial. Many public datasets are outdated or lack detailed ARP-specific information.
- **Feature Engineering**: Identifying the right set of features that can distinguish between legitimate and malicious ARP packets is crucial for model performance.
- **Real-Time Detection**: Ensuring that the model operates efficiently in real-time without introducing latency into the network is a key requirement.

6. Machine Learning-Based Detection

Machine learning-based detection leverages intelligent algorithms to identify ARP spoofing attacks by analyzing patterns in network traffic. Unlike traditional rule-based systems, Machine learning models can learn from historical data and detect both known and unknown attack behaviors. By extracting key features such as

MAC-IP inconsistencies, unusual ARP reply frequencies, and timing anomalies, Machine learning algorithms like SVM, Random Forest, KNN, and XGBoost can accurately differentiate between legitimate and malicious activities. This approach enhances detection accuracy, reduces false positives, and supports real-time monitoring, making it highly effective for securing modern network environments.

7. *Literature Review of Existing Machine Learning Techniques*

This section reviews machine learning techniques for detecting ARP spoofing, a prevalent method for Man-in-the-Middle attacks. Due to spoofing's effectiveness in manipulating network traffic, numerous studies propose Machine Learning-based solutions.

B. A. Mantoo et al., (2022) Proposed the K Nearest Neighbor (KNN) model for the detection of Man-in-the middle attacks KNN model is 0.98 [8].

Morsy & Nashat (2022) Suggested a method of proposed a D-ARP-based detection scheme for man in the middle attacks via ARP spoofing, achieving zero false positives and false negatives [5].

Thankappan et al., (2024) proposed the framework on Raspberry Pea and performed the experiments. we evaluate our framework at different locations in our test case and show that in moderate attacks MC-Man can detect them with an average correctness of 98% [9].

Sivasankari et al., (2022) proposed a regression-based approach for secure routing in Internet of things (IoT) networks. Among LR, MLR, and GPR models, GPR showed the highest attack detection accuracy and lowest misclassification rates[10].

Elmansy et al., (2023) proposed a reinforcement learning-based security model to defend against man in the middle attacks in fog computing. Their approach integrates Software Distributed Network, MPTCP, and MTD to improve network security and resource efficiency [11].

Al-Juboori et al. (2023) proposed utilizing Kaggle website data to establish four machine learning approaches for detecting two common threats that attack connected devices in a network. To verify their capacity to defend devices against such attacks, the analysis revealed over 99% accuracy in MTM identification and over 97% accuracy in Denial of Service identification by all the methods [12].

Majumder et al., (2024) developed a real-time anomaly detection system for a man-made middleman attacker through ARP spoofing, using various machine learning models. The Convictional Neuron Network model achieved an F1- score of 99% in training and 99.26% in real-time detection [13].

Kponyo et al., (2020) demonstrated the use of machine learning based algorithms to detecting the endpoint MIME attacks using Address Resolution Protocol information. On-line classifiers were tested by the authors and this was their detection rate of 99.72% when using machine learning and signal processing techniques [15].

Alani et al., (2023) present a detection technique that employs explainable deep learning to identify Address Resolution Protocol spoofing in the internet of the network.

Disha et al., (2022) The method was designed to address imbalanced data through rescaled class weights and selecting the most informative features[16].

Usmani et al., (2022) presented an LSTM, and Decision Tree classifiers are used in classification. On performing different experiments, we observed that both methods can predict ARP spoofing at 99.9% and 100% accuracy, respectively[17].

M. Ibrahim et al.,(2024) conducted a study on cyber-attack detection and network systems detection and network systems on cyber-attack detection and net systems. System Performance evaluation of the proposed ID model demonstrated high performance, good accuracy, detection rate, and low false alarms [18].

Sebbar et al., (2020) This paper examines a machine learning-based approach for detecting Man in the middle attacks in large-scale software-defined networks [19].

KIKISSAGBE et al., (2024) demonstrate a machine learning method for identifying denial- of-service (DoS) assaults on Internet of Things platforms. The method's effectiveness in identifying denial-of-service attacks is demonstrated. The authors come to the conclusion that IoT systems can be made more secure by using their method [20].

Suvra, (2025) as suggested Special attention was paid to identifying Distributed Denial of Service traffic and mitigating techniques [21].

Tay et al., (2024) focus on Perceptron, Random Forest. This work does not address man-in- the-middle attacks. The article is dedicated to Distributed Denial of Service detection methods and their evaluation [22].

Satyanegara et al., (2022) engage in the detection of human attacks on MLP and CNN- MSTM. We are investigated various methods of scaling up the functions and got the best results of 99.74% in the CNN-MLP model in the machine learning techniques [23].

In Rajput et al. (2023), the main focus is on the evaluation of several machines. These machines were assessed for their efficiency and reliability in various operational scenarios. The findings suggest significant improvements in performance metrics, indicating potential advancements in the field [24].

D. Jim Solomon Raja (2024) describes an Intrusion Detection System (IDS) based on machine learning (ML) that can identify Man-in-the-Middle (MITM) attacks in a smart grid (SG) advanced metering infrastructure (AMI). The proposed system leverages various algorithms to analyze network traffic patterns, enabling it to detect anomalies indicative of such attacks. By continuously learning from new data, the IDS enhances its accuracy and response time, significantly improving the overall security of the smart grid infrastructure [25].

M. Usmani et al. (2022) Explores using Machine Learning (ML) and Deep Learning (DL) to detect ARP spoofing attacks in sensor networks, which are vulnerable to various threats like DoS and Man-in-the-Middle attacks. Long Short-Term Memory networks and decision tree classifiers were employed for early attack prediction and evaluated on a comprehensive dataset. The results demonstrated a significant improvement in detection accuracy compared to traditional methods, highlighting the potential of these advanced techniques in enhancing network security. Future research may focus on optimizing these models further and applying them to real-time monitoring systems [17].

H. Mohapatra (2020) enhances the security problem to identifying, isolating, and reconfiguring attacked nodes using a Man in the Middle-Intrusion Detection System (MITM-IDS) for wireless sensor networks (WSN). This system employs advanced algorithms to analyze traffic patterns and identify anomalies that may indicate a potential attack. By effectively isolating compromised nodes, it ensures the integrity and reliability of the overall network, providing a robust defense against intrusions [26].

D. Abreu et al., (2022) propose an online attack detection system on network traffic classification that combines experimental network machine learning, deep learning, and ensemble learning techniques. By applying multi-level data analytics, the system can continuously monitor network traffic, identify malicious flows in real time and accurately classify them based on the specific type of attack. This hybrid approach enhances detection accuracy and supports timely response to evolving threats in a dynamic network environment[27].

J. Wigchert, S. (2025) Shows that, in contrast to state-of-the-art techniques, their suggested method can accurately detect Low Earth Orbit (LEO) spoofing attacks delivered from a variety of altitudes. Given the ever-changing nature of satellite-based threats, their strategy demonstrates a high degree of adaptability. They have also made their gathered dataset publicly available as open source, which promotes more study and advancement in the area of satellite security[28].

Z. Liu et al., (2023) In this learning method by the machine was able to automatically detect differences between normal data and abnormal data with high accuracy. Furthermore, generalized machine learning methods are robust and can detect unknown attacks as well. Deep learning is a branch of machine learning whose performance is impressive and has become an area of research [29].

A. Alsaaidah et al.,(2024) Study is to demonstrate how algorithmic performance provides a range of solutions that satisfy different quality requirements, albeit at the price of speed and accuracy. Numerous algorithms were evaluated to determine the optimal trade-off between processing time and result accuracy [30].

8. Comparison Table

Table 1 describes various method used, limitations performance parameters of previous research. In this survey paper, we've studied various methods of Machine learning techniques ARP spoofing attack. Several studies have used machine learning for Address Resolution Protocol (ARP) spoofing detection within network intrusion research. Models like SVM, random forests, and neural networks analyze packet features to spot anomalies. ML helps detect attacks more accurately than rule-based methods.

No	Author's	Method used	Limitations	Parameters
1.	B. A. Mantoo and P. Kaur (2022)	K Nearest Neighbor (KNN)	Attacker's dynamically changes their behavior to avoid detection.	The accuracy is 0.98.
2.	Suvra, D. (2025).	LR, KNN, RF, SVM, NB, DT	Hybrid classifier: limited to accuracy enhancement	DT: 98.50% accuracy, RF: 98.80% accuracy

3.	Tay et al., 2024	KNN, MP, RF	Future research may explore larger datasets.	99.35%/90.63% RF binary classification.
4.	Morsy, (2022).	DHCP server Nmap for MAC detection.	Centralized servers: single point of failure.	Zero false positives /negatives ARP spoofing attack.
5.	Al- Juboori (2023).	Random forest (RF),XGB (xgboost),GB Decision Tree	Need broader attack data	99% MITM, 97% DoS accuracy.
6.	Satyanega (2022)	CNN-MLP CNN-LSTM	Lack of comparison with more recent techniques.	99.74% (Standard Scalar), CNN-LSTM: 99.74% to 99.57%.
7.	Rajput, (20 23).	DT, RF, GB, KNN	IDS: detecting novel attacks is difficult.	Evaluated ML attack detection.
8.	Arul (2023)	Gaussian Naive Bayes (GNB)	Limited Internet of thing environment adaptability.	Detection probability: 99.6% (GNB).
9.	Sivasankar (2022)	LR MLR GPR	Latency/encryption impacts detection.	GPR: higher MITM detection than LR/MLR.
10.	Ismail (2023)	DNN	Software Distributed Network deployment: increased DNN resource cost.	Arp-probe: 0.999 F1, 0.026% FPR, 0.001% FNR.
11.	Elmansy (2023)	RL MPTCP MTD SDN	Simulation-based evaluation only.	Mininet simulation experiments.
12.	Kponyo, (2020)	linear-based ML Classification Models	Limited by evolution/compute.	High efficiency, 99.72% accuracy.
13.	Majumder, (2024)	KNN, DT, RF, ANN, DNN	Scalability, network, attack adaptability limits.	99% F1-Score, 99.26% training accuracy CNN attack detection.
14.	Bilal Ahmad (2022)	KNN Wireshark	Controlled data limits evaluation	Accuracy: 98%.
15.	Ibrahim &(2024)	LSTM	High computational requirements, not optimized for real-time detection	Achieved 88.4%
16.	Solomon 2024	Effectively identifies MITM attacks in smart grid AMI.	Limited scalability to large-scale smart grid environments. Focuses only on MITM attacks, not other cyber threats.	Hybrid Bat Algorithm (HBA) optimizes RF performance.
17.	Usmani 2022	LSTM	The reliance on a specific dataset may also limit generalizability.	LSTM achieved 99% accuracy, while the decision tree reached 100%.
18.	Mohapatra 2020	Machine Learning-Based Classification	Training nodes for attack detection may increase resource consumption.	Simulation results show 89.15%

Table 1: Comparison of Existing work

9. Conclusion

This review paper validates the substantial potential of Machine Learning in Address Resolution Protocol Spoofing-based man-in-the-middle attack detection and prevention. A systematized exploration of the

various Machine Learning models, including supervised, unsupervised, and deep learning, has been established to identify anomalous Address Resolution Protocol traffic. Feature selection is critical to detection, and the quality of datasets, as well as real-time processing, are important to detection. The realization of deployment barriers, such as data preprocessing, model optimization, and class imbalance, is essential to the application. This research provides an insight into the role of Machine Learning in network security. It is essential to continue research to refine these methods in the face of ever-changing cyber threats. The realization of a Machine Learning solution will increase security and reduce the risk of an Address Resolution Protocol spoofing attack.

The review clearly demonstrates that machine learning holds considerable promise for detecting and mitigating ARP spoofing-based Man-in-the-Middle attacks. Across the surveyed studies, both traditional supervised models and advanced deep learning architectures have achieved impressive detection rates, with some exceeding 99% accuracy under controlled conditions.

However, the results also highlight important caveats. High accuracy in a laboratory does not guarantee robustness in live, large-scale network environments. Real-world deployment introduces challenges such as imbalanced datasets, processing latency, and the continuous evolution of attack strategies. These factors underscore the importance of model adaptability, robust feature selection, and real-time performance optimization.

10.Reference

[1] C. Garzon, A. Lahmadi, J. Vergara, A. Leal, and J. F. Botero, “In-Band ARP-based Man-in-the-Middle Attack Detection Using P4 Programmable Switches,” *2024 IEEE Latin-American Conf. Commun. LATINCOM 2024 - Proc.*, pp. 2024–2025, 2024, doi: 10.1109/LATINCOM62985.2024.10770688.

[2] H. Bazzi, A. Nassar, M. El Bizri, and A. M. H. Prof, “A PRACTICAL INTRUSION DETECTION APPROACH FOR ARP,” vol. 6, no. 1, 2024.

[3] A. A. Tadesse, “A Thesis Prepared By: Abel Ashenafi Tadesse,” 2022.

[4] J. Kim, J. Park, and J. H. Lee, “Simulation of an ARP Spoofing Attack on the E2 Interface in Open RAN,” *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, pp. 2024–2025, 2024, doi: 10.1109/PIMRC59610.2024.10817456.

[5] S. M. Morsy and D. Nashat, “D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing,” *IEEE Access*, vol. 10, no. May, pp. 49142–49153, 2022, doi: 10.1109/ACCESS.2022.3172329.

[6] M. Alwazzeh, S. Karaman, and M. N. Shamma, “Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat,” *J. Cyber Secur. Mobil.*, no. July, 2020, doi: 10.13052/jcsm2245-1439.933.

[7] Amrit Kaur, “Detection of Phishing Websites Using SVM Technique,” *Imp. J. Interdiscip. Res.*, vol. 2, no. 8, pp. 1273–1276, 2016.

[8] B. A. Mantoo and P. Kaur, “A Machine Learning Model for Detection of Man in The Middle Attack Over Unsecured Devices,” *AIP Conf. Proc.*, vol. 2555, no. February, pp. 0–10, 2022, doi: 10.1063/5.0109151.

[9] M. Thankappan, H. Rifà-Pous, and C. Garrigues, “A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks,” *Int. J. Inf. Secur.*, vol. 23, no. 6, pp. 3527–3546, 2024, doi: 10.1007/s10207-024-00899-9.

[10] N. Sivasankari and S. Kamalakkannan, “Detection and prevention of man-in-the-middle attack in iot network using regression modeling,” *Adv. Eng. Softw.*, vol. 169, no. February, p. 103126, 2022, doi: 10.1016/j.advengsoft.2022.103126.

[11] H. Elmansy, K. Metwally, and K. Badran, “Reinforcement learning-based security schema mitigating man-in-the-middle attacks in fog computing,” *Int. J. Electr. Comput. Eng.*, vol. 13, no. 5, pp. 5908–5921, 2023, doi: 10.11591/ijece.v13i5.pp5908-5921.

[12] S. A. M. Al-Juboori, F. Hazzaa, Z. S. Jabbar, S. Salih, and H. M. Gheni, “Man-in-the-middle and denial of service attacks detection using machine learning algorithms,” *Bull. Electr. Eng. Informatics*, vol. 12, no. 1, pp. 418–426, 2023, doi: 10.11591/eei.v12i1.4555.

[13] S. Majumder, M. K. Deb Barma, and A. Saha, *ARP spoofing detection using machine learning classifiers: an experimental study*, vol. 67, no. 1. Springer London, 2024. doi: 10.1007/s10115-024-02219-y.

[14] M. M. Alani, A. I. Awad, and E. Barka, “ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning,” *Internet of Things (Netherlands)*, vol. 23, no.

February, 2023, doi: 10.1016/j.iot.2023.100861.
[15] J. J. Kponyo, J. O. Agyemang, and G. S. Klogo, "Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 3, pp. 384–388, 2020, doi: 10.17762/ijcnis.v12i3.4735.
[16] R. A. Disha and S. Waheed, "Performance analysis of machine learning models for intrusion detection system using Gini Impurity-based Weighted Random Forest (GIWRF) feature selection technique," *Cybersecurity*, vol. 5, no. 1, pp. 1–22, 2022, doi: 10.1186/s42400-021-00103-8.
[17] M. Usmani, M. Anwar, K. Farooq, G. Ahmed, and S. Siddiqui, "Predicting ARP spoofing with Machine Learning," *2022 Int. Conf. Emerg. Trends Smart Technol. ICETST 2022*, no. September 2022, 2022, doi: 10.1109/ICETST55735.2022.9922925.
[18] M. Ibrahim and R. Elhafiz, "Modeling an intrusion detection using recurrent neural networks," *J. Eng. Res.*, vol. 11, no. 1, p. 100013, 2023, doi: 10.1016/j.jer.2023.100013.
[19] A. Sebbar, K. Zkik, Y. Baddi, M. Boulmalf, and M. D. E. C. El Kettani, "MitM detection and defense mechanism CBNA-RF based on machine learning for large-scale SDN context," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 12, pp. 5875–5894, 2020, doi: 10.1007/s12652-020-02099-4.
[20] B. R. KIKISSAGBE, M. Adda, P. Célicourt, I. T. HAMAN, and A. Najjar, "Machine Learning for DoS Attack Detection in IoT Systems," *Procedia Comput. Sci.*, vol. 241, no. 2019, pp. 195–202, 2024, doi: 10.1016/j.procs.2024.08.027.
[21] D. K. Suvra, "An Efficient Real Time DDoS Detection Model Using Machine Learning Algorithms," 2025, [Online]. Available: http://arxiv.org/abs/2501.14311
[22] W. Tay, S. Chong, and L. Chong, "DDoS Attack Detection with Machine Learning," vol. 3, no. 3, 2024.
[23] H. H. Satyanegara and K. Ramli, "Implementation of CNN-MLP and CNN-LSTM for MitM Attack Detection System," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 6, no. 3, pp. 387–396, 2022, doi: 10.29207/resti.v6i3.4035.
[24] M. A. Rajput, Muhammad Umar, A. Ahmed, Ali Raza Bhangwar, Khadija Suhail Memon, and Misbah, "Evaluation of Machine Learning based Network Attack Detection," *Sukkur IBA J. Emerg. Technol.*, vol. 5, no. 2, pp. 57–66, 2023, doi: 10.30537/sjet.v5i2.1186.
[25] D. Jim Solomon Raja, R. Sriranjani, P. Arulmozhi, and N. Hemavathi, "Unified Random Forest and Hybrid Bat Optimization Based Man-in-the-Middle Attack Detection in Advanced Metering Infrastructure," *IEEE Trans. Instrum. Meas.*, vol. 73, pp. 1–12, 2024, doi: 10.1109/TIM.2024.3420375.
[26] H. Mohapatra, "Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System," *Int. J. Emerg. Trends Eng. Res.*, vol. 8, no. 5, pp. 1503–1510, 2020, doi: 10.30534/ijeter/2020/05852020.
[27] D. Abreu and A. Abelem, "OMINACS: Online ML-Based IoT Network Attack Detection and Classification System," *2022 IEEE Latin-American Conf. Commun. LATINCOM 2022*, 2022, doi: 10.1109/LATINCOM56090.2022.10000544.
[28] J. Wigchert, S. Sciancalepore, and G. Oligeri, "Detection of Aerial Spoofing Attacks to LEO Satellite Systems via Deep Learning," *Comput. Networks*, vol. 269, pp. 1–11, 2025, doi: 10.1016/j.comnet.2025.111408.
[29] Z. Liu, J. Hu, Y. Liu, K. Roy, X. Yuan, and J. Xu, "Anomaly-Based Intrusion on IoT Networks Using AIGAN-a Generative Adversarial Network," *IEEE Access*, vol. 11, no. August, pp. 91116–91132, 2023, doi: 10.1109/ACCESS.2023.3307463.
[30] A. Alsaaidah, O. Almomani, A. A. Abu-Shareha, M. M. Abualhaj, and A. Achuthan, "ARP Spoofing Attack Detection Model in IoT Networks Using Machine Learning: Complexity vs. Accuracy," *J. Appl. Data Sci.*, vol. 5, no. 4, pp. 1850–1860, 2024, doi: 10.47738/jads.v5i4.374.
[31] K. Uszko, M. Kasprzyk, M. Natkaniec, and P. Chołda, "Rule-Based System with Machine Learning Support for Detecting Anomalies in 5G WLANs," *Electron.*, vol. 12, no. 11, 2023, doi: 10.3390/electronics12112355.