International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Defending Against Arpspoofing In Wifi Networks Using Rf Fingerprinting

Ms.K.Madhunitha [1], Bharath K [2,] Deva Senathipathi M [3], Mukilan R [4]

[1] Assistant Professor Department of Computer Science and Engineering Kongunadu College of Engineering and Technology Tamilnadu,India

[2 3 4] Department of Computer Science and Engineering Kongunadu College of Engineering and Technology Tamilnadu,India

Abstract- — Address Resolution Protocol (ARP) spoofing is a critical security threat in wireless networks where an attacker sends forged ARP messages to link their device with the IP address of a legitimate user. This attack allows malicious users to intercept, modify, or block data traffic between communicating devices, leading to serious issues such as data theft, session hijacking, and denial-of-service attacks. Traditional detection mechanisms mainly rely on software-based identifiers such as IP addresses and MAC addresses. However, these identifiers can be easily manipulated by attackers, making conventional solutions less effective in detecting sophisticated attacks. To overcome this limitation, this study proposes a defense mechanism against ARP spoofing in Wi-Fi networks using Radio Frequency (RF) fingerprinting. RF fingerprinting identifies wireless devices based on unique hardware-level characteristics of their transmitted signals. Features such as frequency offset, phase noise, and signal transient patterns are analyzed to generate distinct RF signatures for each device. The proposed system continuously monitors wireless transmissions and compares them with stored RF fingerprints to identify anomalies and detect unauthorized devices. By leveraging physical layer characteristics, the approach provides a reliable and difficult-to-forge method of authentication. Experimental results indicate that RF fingerprinting significantly improves the accuracy of ARP spoofing detection and strengthens overall wireless network security without requiring major modifications to existing infrastructure.

Keywords:- ARP Spoofing, Wi-Fi Security, RF Fingerprinting, Network Intrusion Detection, Wireless Network Protection, Device Authentication.

I. INTRODUCTION

Wireless networks have become an essential component of modern communication systems, enabling users to access the internet and share data conveniently through Wi-Fi technology. These networks are widely used in homes, educational institutions, offices, and public environments due to their flexibility and ease of deployment. However, the open nature of wireless communication makes Wi-Fi networks vulnerable to various security threats and cyberattacks. One of the most common and dangerous attacks in local area networks is Address Resolution Protocol (ARP) spoofing. In this attack, a malicious user sends forged ARP messages within the network to associate their device's MAC address with the IP address of a legitimate device. As a result, network traffic intended for the legitimate device is redirected to the attacker, enabling them to monitor, manipulate, or block communication between network nodes.

ARP spoofing can lead to several serious consequences, including data interception, man-in-the-middle attacks, session hijacking, and denial-of-service conditions. Traditional network security mechanisms mainly rely on logical identifiers such as IP addresses and MAC addresses to verify device authenticity. However, these identifiers can easily be altered or spoofed by attackers, making conventional detection techniques less effective in preventing sophisticated attacks. Therefore, more reliable and robust methods are required to improve the security of wireless networks.

Radio Frequency (RF) fingerprinting has emerged as a promising technique for device identification and authentication at the physical layer of wireless communication. Every wireless device possesses unique hardware characteristics due to slight imperfections in its radio transmitter components. These imperfections generate distinct patterns in the transmitted RF signals, such as variations in frequency offset, phase noise, and signal transients. RF fingerprinting analyzes these unique signal characteristics to create a specific signature for each device. Since these hardware-based features are difficult to replicate or modify, RF fingerprinting provides a strong mechanism for identifying legitimate devices and detecting unauthorized ones.

In this context, the proposed approach focuses on defending against ARP spoofing attacks in Wi-Fi networks by using RF

fingerprinting techniques. By continuously monitoring wireless transmissions and comparing signal features with stored RF signatures, the system can detect anomalies and identify malicious devices attempting to spoof network identities. This approach enhances the reliability of intrusion detection mechanisms and strengthens overall wireless network security without requiring significant changes to the existing infrastructure.

II. RELATED WORKS

Detection and Prevention of ARP Spoofing Attacks: Gunjan Agrawal focuses on the vulnerabilities of the Address Resolution Protocol (ARP) and the security risks caused by ARP spoofing attacks in computer networks. ARP spoofing occurs when an attacker sends fake ARP messages to associate their MAC address with a legitimate IP address, enabling them to intercept network traffic. The paper analyzes how attackers exploit ARP weaknesses to perform man-in-the-middle attacks, session hijacking, and data interception. The author proposes detection and prevention mechanisms using network monitoring and intrusion detection techniques. The study explains the limitations of the ARP protocol, which lacks authentication and therefore allows malicious users to manipulate ARP tables easily. Various security tools and techniques are evaluated to identify abnormal ARP packets and prevent spoofing attempts. The research highlights the importance of implementing secure monitoring systems in local networks to detect suspicious traffic patterns. It concludes that effective ARP spoofing detection mechanisms are necessary to protect network communication and ensure data integrity.

ARP Spoof Detection and Mitigation: Prema Arokiya Mary, Sanjay M. S., Vijayasenthil E., Abdur Rahman K., Sabari B. presents a comprehensive method for detecting and mitigating ARP spoofing attacks in local networks. The authors explain that ARP spoofing is a serious security threat that allows attackers to intercept and manipulate communication between network devices. The proposed system monitors ARP traffic and identifies suspicious packets by analyzing inconsistencies between IP and MAC address mappings. The paper describes the design of a detection mechanism that compares ARP responses with stored network information to identify anomalies. Once an attack is detected, the system alerts administrators and blocks malicious communication. The research highlights the importance of real-time monitoring and automated mitigation techniques to protect networks from unauthorized access. Experimental results show that the proposed system improves network security by quickly identifying spoofed ARP packets and preventing further attacks. The study concludes that effective ARP monitoring tools can significantly reduce the risk of man-in-the-middle attacks and improve overall network reliability.

Detecting and Preventing ARP Spoofing Attacks Using Real-Time Data Analysis and Machine Learning: Mrinal Kumar, Chandra Sekhar Dash introduces a machine learning–based approach for detecting ARP spoofing attacks in computer networks. The authors propose using advanced algorithms such as Random Forest, Support Vector Machines (SVM), Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Isolation Forest to analyze ARP traffic patterns. The system collects network traffic data and extracts relevant features to identify malicious activities. By training machine learning models on normal and attack datasets, the system can detect abnormal behavior in real time. The study evaluates the performance of each algorithm using metrics such as accuracy, precision, recall, and F1-score. Experimental results demonstrate that machine learning techniques significantly improve detection accuracy compared to traditional rule-based methods. The research highlights the importance of intelligent security mechanisms in modern networks where attacks are becoming increasingly sophisticated. The proposed approach enhances network security by providing faster detection and automated prevention of ARP spoofing attacks.

Study of Vulnerabilities of ARP Spoofing and Its Detection Using SNORT: Rajneet Kaur Bijral, Alka Gupta, Lalit Sen Sharma investigates the vulnerabilities associated with ARP spoofing attacks and proposes the use of the SNORT intrusion detection system for identifying such threats. The authors explain that ARP spoofing exploits weaknesses in the ARP protocol to redirect network traffic through a malicious device. This enables attackers to perform activities such as packet sniffing, session hijacking, and unauthorized data access. The study analyzes how SNORT can be configured to monitor ARP packets and detect suspicious patterns in network communication. By creating specific detection rules, the system identifies abnormal ARP responses and alerts administrators about potential attacks. The research includes experimental evaluations conducted on real network environments to assess the effectiveness of the proposed method. Results indicate that intrusion detection systems like SNORT can significantly improve network security by identifying spoofing attempts early. The paper emphasizes the need for continuous monitoring and automated detection tools in modern network infrastructures.

A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting: Wenbo Wang, Ignacio Aguilar reviews various techniques used for detecting spoofing attacks

through radio frequency fingerprinting. RF fingerprinting identifies devices based on unique hardware characteristics present in transmitted wireless signals. These physical layer features include frequency offset, signal distortion, and phase noise. The authors discuss how RF fingerprinting can distinguish legitimate transmitters from malicious ones, making it useful for detecting spoofing and jamming attacks in wireless systems. The paper also examines the challenges associated with implementing RF fingerprinting techniques, such as noise interference and environmental variations. Different feature extraction methods and classification algorithms are analyzed to improve device identification accuracy. The study highlights that RF fingerprinting can provide an additional layer of authentication beyond traditional network security mechanisms. The authors conclude that physical-layer identification techniques are promising solutions for protecting wireless networks from spoofing attacks.

Stay Connected, Leave No Trace: Enhancing Security and Privacy in Wi-Fi via Obfuscating Radiometric Fingerprints: Luis F. Abanto-Leon, Andreas Baeuml, Gek Hong Sim, Matthias Hollick, Arash Asadi explores the use of radiometric fingerprinting to enhance security and privacy in wireless networks. Radiometric fingerprints are unique patterns generated by hardware imperfections in wireless transmitters. These fingerprints can be used to identify and authenticate devices in a network. The authors propose a system called RF-Veil that modifies transmitted signals in a controlled manner to protect user privacy while still allowing legitimate receivers to verify device identity. The paper demonstrates how radiometric fingerprints can be used to detect spoofed devices and prevent unauthorized access in Wi-Fi networks. Experimental evaluations show that the proposed system effectively protects devices from impersonation attacks while maintaining communication performance. The research highlights the importance of combining physical-layer authentication with traditional network security mechanisms to strengthen wireless network protection.

Generative Adversarial Network for Wireless Signal Spoofing: Yi Shi, Kemal Davaslioglu, Yalin E. Sagduyu investigates the use of deep learning techniques for generating spoofed wireless signals that can imitate legitimate transmissions. The authors propose a system based on Generative Adversarial Networks (GANs) that can create synthetic wireless signals to deceive device identification systems. The study examines how attackers can exploit machine learning methods to bypass RF fingerprinting defenses. The proposed model includes a generator that creates fake signals and a discriminator that evaluates whether the signals appear legitimate. Through iterative training, the generator improves its ability to mimic authentic wireless transmissions. The research highlights potential security risks associated with wireless signal authentication techniques. At the same time, it demonstrates how deep learning can also be used to strengthen defensive systems against spoofing attacks. The findings emphasize the need for robust security mechanisms that can detect sophisticated signal-level attacks in wireless networks.

ARP-PROBE: ARP Spoofing Detection Using Explainable Deep Learning introduces ARP-PROBE, a deep learning-based system designed to detect ARP spoofing attacks in Internet of Things (IoT) networks. The system analyzes network packets and extracts important features related to ARP communication patterns. These features are then processed using deep learning models to classify normal and malicious network behavior. The authors incorporate explainable artificial intelligence techniques to help administrators understand how the model identifies spoofing attacks. Experimental evaluations show that ARP-PROBE achieves extremely high accuracy in detecting ARP spoofing attacks, reaching nearly perfect classification performance. The study highlights the growing importance of intelligent detection systems in IoT environments where traditional security mechanisms are insufficient. The proposed approach improves network protection by providing accurate and interpretable attack detection methods that can be deployed in real-time monitoring systems.

Collusion-Driven Impersonation Attack on Channel-Resistant RF Fingerprinting: Zhou Xu, Guyue Li, Zhe Peng, Aiqun Hu investigates advanced attacks targeting RF fingerprinting-based authentication systems. The authors propose a collusion-driven impersonation attack that attempts to replicate the RF fingerprint of a legitimate device. By synchronizing with a collaborating receiver and adjusting signal characteristics, attackers can mimic the spectral features of genuine transmitters. The paper analyzes how such attacks can challenge the reliability of RF fingerprinting methods used for wireless security. The authors also propose improved detection techniques that enhance the robustness of RF fingerprinting systems against impersonation attempts. Simulation results demonstrate that the proposed attack can achieve high success rates under different channel conditions, highlighting potential vulnerabilities in existing RF fingerprinting solutions. The study emphasizes the importance of designing more resilient device authentication mechanisms to defend against sophisticated spoofing attacks.

Protocol-Agnostic Backdoor Attacks on RF Fingerprinting Models: Tianya Zhao, Ningning Wang, Junqing Zhang, Xuyu Wang explores vulnerabilities in machine learning models used

for RF fingerprinting-based device authentication. The authors investigate how attackers can introduce hidden backdoors into pre-trained models without requiring access to training data. By embedding specific triggers in the model, attackers can manipulate the classification process and bypass authentication mechanisms. The research demonstrates that such backdoor attacks can affect multiple RF fingerprinting tasks across different communication protocols. Experimental results show that compromised models may incorrectly identify malicious devices as legitimate transmitters. The paper also discusses potential countermeasures to detect and mitigate these attacks. The study highlights the importance of secure machine learning practices when implementing RF fingerprinting systems for wireless network protection.

III. PROPOSED METHOD

The proposed system is designed to protect Wi-Fi networks from ARP spoofing attacks by applying Radio Frequency (RF) fingerprinting for reliable device identification. Traditional security mechanisms mainly depend on logical identifiers such as IP addresses and MAC addresses to verify devices in a network. However, these identifiers can easily be forged or manipulated by attackers, making conventional ARP-based protection techniques less effective. To address this problem, the proposed method utilizes the physical characteristics of wireless signals to authenticate devices connected to the network.

In this system, a monitoring unit continuously observes wireless transmissions within the Wi-Fi environment. The captured signals are processed to extract distinctive RF features including frequency offset, phase noise, amplitude variations, and transient signal behavior. These parameters reflect the unique hardware characteristics of each wireless device and are used to generate a specific RF fingerprint. During the initial setup phase, the fingerprints of authorized devices are recorded and stored in a secure database to create a reference dataset for future comparison.

Whenever a device communicates in the network, the system extracts its RF signal characteristics and compares them with the stored fingerprints. If the features match a registered profile, the device is recognized as legitimate and allowed to continue communication. If the fingerprint does not correspond to any stored profile, the system identifies the device as suspicious and marks it as a potential ARP spoofing attacker. In such cases, the system can generate alerts and take preventive actions such as blocking or isolating the malicious device.

By integrating RF fingerprint analysis with ARP traffic monitoring, the proposed system provides an additional layer of security at the physical level. This approach improves the accuracy of attack detection and strengthens overall wireless network protection without requiring major modifications to the existing infrastructure.

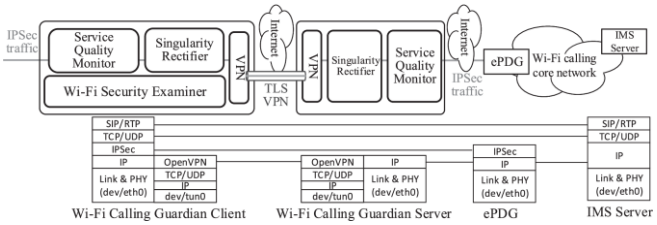

Figure.1.System Architecture

The proposed system for defending against ARP spoofing in Wi-Fi networks using RF fingerprinting is organized into several functional modules that work together to detect and prevent malicious activities. Each module performs a specific task to ensure accurate device identification and secure network communication.

Network Monitoring Module
This module continuously monitors all wireless communications within the Wi-Fi network. It captures packets transmitted by different devices and observes ARP requests and responses exchanged between nodes. The monitoring system records relevant information such as IP addresses, MAC addresses, and packet transmission patterns. By maintaining real-time observation of network traffic, this module provides the necessary data for detecting abnormal activities and possible ARP spoofing attempts.

RF Signal Capture and Feature Extraction Module
In this module, wireless signals transmitted by devices are captured and analyzed. Important physical-layer characteristics such as frequency offset, phase noise, amplitude variations, and signal transient behavior are extracted from the RF signals. These features represent the hardware-level imperfections of wireless transmitters and serve as unique identifiers for each device.

RF Fingerprint Database Module
The extracted RF features of legitimate devices are stored in a centralized database as reference fingerprints. During the system initialization phase, the system collects RF signatures from authorized devices and saves them securely. This database

acts as a baseline for comparing newly observed signals and identifying whether a device is genuine or suspicious.

Device Authentication and Attack Detection Module
This module compares the RF fingerprint of an incoming signal with the stored fingerprints in the database. If the fingerprint matches a registered profile, the device is authenticated as legitimate. If there is a mismatch, the system detects the presence of a suspicious device and identifies it as a potential ARP spoofing attacker.

Alert and Prevention Module
Once a malicious device is detected, this module generates alerts for network administrators and takes appropriate preventive actions. These actions may include blocking the attacker's communication, isolating the device from the network, or updating the security logs. This ensures that the network remains secure and protected from ARP spoofing attacks.

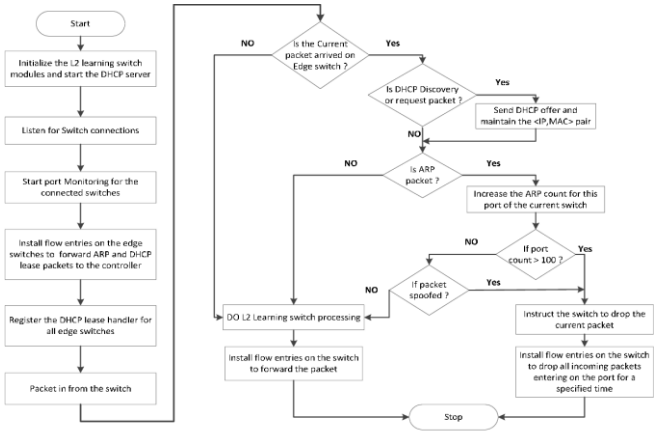

Figure.2.Methodology workflow of the ARFspoofing in Wifi Networks Using RF Fingerprinting Framework

Overall Working Flow of the Proposed System:
The proposed system for defending against ARP spoofing in Wi-Fi networks using RF fingerprinting follows a structured workflow to detect and prevent malicious activities in wireless communication. The system integrates network monitoring, radio frequency (RF) feature extraction, device identification, and attack detection to ensure secure communication between devices in a wireless environment.

Initially, the system continuously monitors the Wi-Fi network and captures network packets, particularly Address Resolution Protocol (ARP) packets transmitted between devices. ARP packets are analyzed because attackers commonly exploit this protocol to perform spoofing attacks by sending fake ARP replies and associating their MAC address with a legitimate IP address. During the packet capture phase, both the network-level information and the physical layer signals are collected from transmitting devices.

In the next stage, RF fingerprinting is applied to extract unique physical layer characteristics from the wireless signals of each device. These characteristics include signal strength variations, frequency offsets, modulation errors, and other hardware-based imperfections that naturally occur in wireless transmitters. Since these features are unique for each device, they serve as reliable identifiers similar to digital fingerprints.

After feature extraction, the system stores the RF fingerprints of legitimate devices in a secure database during a training or registration phase. Machine learning algorithms are then used to build classification models that can accurately identify authorized devices based on their RF signatures.

During real-time operation, incoming packets are analyzed and their RF fingerprints are compared with the stored fingerprints of legitimate devices. If a packet claims a legitimate MAC or IP address but its RF fingerprint does not match the registered device profile, the system identifies it as a potential ARP spoofing attack.

Finally, once an attack is detected, the system generates alerts and blocks the malicious device from communicating within the network. This workflow ensures continuous monitoring, accurate device identification, and effective protection against ARP spoofing attacks in Wi-Fi networks.

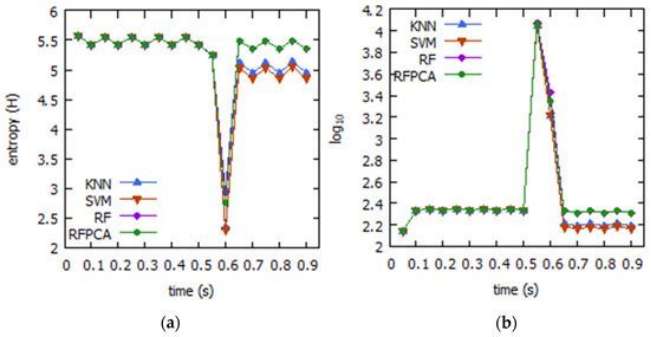

Figure.3.Performance Evaluation of ARFspoofing in Wifi Networks Using RF Fingerprinting Framework

$$D = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

Euclidean distance is widely used in RF fingerprinting systems to measure the similarity between two feature vectors extracted from wireless signals. In Equation (1), x_irepresents the RF feature value of a received signal, while y_idenotes the corresponding feature value stored in the database for a legitimate device. The variable nindicates the total number of extracted RF features. The calculated distance value determines how closely the received signal matches the stored fingerprint. If the distance is small, the device is considered legitimate. However, a larger distance indicates that the signal originates from a different transmitter, helping the system detect potential ARP spoofing attacks.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Accuracy is a commonly used performance evaluation metric in classification systems. In Equation (4), TP(True Positive) represents correctly detected attacks, TN(True Negative) represents correctly identified legitimate devices, FP(False Positive) represents legitimate devices incorrectly classified as attackers, and FN(False Negative) represents undetected spoofing attacks. The accuracy value indicates the overall effectiveness of the ARP spoofing detection system. A higher accuracy value signifies that the system correctly distinguishes between legitimate and malicious devices. In RF fingerprint-based security systems, this metric is essential for evaluating the reliability and efficiency of the proposed detection mechanism.

V. FUTURE WORK

Future work for the proposed system of defending against ARP spoofing in Wi-Fi networks using RF fingerprinting can focus on improving detection accuracy, scalability, and real-time implementation. One important enhancement is the integration of advanced machine learning and deep learning algorithms, such as convolutional neural networks and recurrent neural networks, to improve the classification of RF fingerprints. These techniques can capture more complex signal patterns and increase the reliability of device identification in dynamic wireless environments.

Another potential improvement is the expansion of the RF fingerprint database to include a larger number of devices operating under different environmental conditions. Factors such as signal interference, mobility, and varying transmission power can influence RF characteristics, and addressing these factors will help build a more robust detection model. Additionally, incorporating adaptive learning techniques can allow the system to continuously update device fingerprints and improve detection performance over time.

Future research can also focus on implementing the proposed system in real-world large-scale wireless networks such as campus networks, smart homes, and IoT environments. Integrating the system with existing network security frameworks and intrusion detection systems will further strengthen protection against spoofing attacks. Ensuring efficient processing and minimal network overhead will also be essential for practical deployment.

REFERENCES

1. W. Wang, I. Aguilar Sanchez, G. Caparra, A. McKeown, T. Whitworth, and E. S. Lohan, “A survey of spoofer detection techniques via radio frequency fingerprinting with focus on the GNSS pre-correlation sampled data,” Sensors, vol. 21, no. 9, pp. 1–24, 2021.
2. J. Machaj, C. Safon, S. Matúška, and P. Brída, “Detection of access point spoofing in the Wi-Fi fingerprinting based positioning,” Sensors, vol. 24, no. 23, pp. 1–19, 2024.
3. Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, “Generative adversarial network for wireless signal spoofing,” arXiv preprint, 2019.
4. L. F. Abanto-Leon, A. Baeuml, G. H. Sim, M. Hollick, and A. Asadi, “Stay connected, leave no trace: Enhancing security and privacy in Wi-Fi via obfuscating radiometric fingerprints,” IEEE Trans. Mobile Computing, 2020.
5. S. Gopalakrishnan, M. Cekic, and U. Madhow, “Robust wireless fingerprinting via complex-valued neural networks,” IEEE Wireless Communications Letters, 2019.
6. G. Agrawal, “Detection and prevention of ARP-spoofing attacks,” International Journal of Engineering Research & Technology, vol. 8, no. 10, pp. 1–5, 2019.
7. M. Kumar and C. S. Dash, “Detecting and preventing ARP spoofing attacks using real-time data analysis and machine learning,” International Journal of Innovative Research in Computer Science and Technology, vol. 11, no. 2, pp. 45–52, 2023.
8. R. K. Bijral, A. Gupta, and L. S. Sharma, “Study of vulnerabilities of ARP spoofing and its detection using SNORT,” International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 123–128, 2017.

9. J. Singh and V. Grewal, "A survey of different strategies to pacify ARP poisoning attacks in wireless networks," International Journal of Computer Applications, vol. 116, no. 11, pp. 25–28, 2015.
10. A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1851–1877, 2019.
11. Y. Xiao, X. Shen, and D. Z. Du, Wireless Network Security. Springer, 2007.
12. S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM Computer Communication Review, vol. 19, no. 2, pp. 32–48, 1989.
13. D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography. Stanford University, 2020.
14. A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," IEEE Symposium on Security and Privacy, pp. 56–73, 2000.
15. Y. W. Law, M. Palaniswami, L. Van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer security in wireless sensor networks," ACM Transactions on Sensor Networks, vol. 1, no. 2, pp. 289–321, 2005.
16. A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," Advances in Neural Information Processing Systems, 2017.
17. I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.
18. A. Graves, A. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," IEEE ICASSP, pp. 6645–6649, 2013.
19. Y. Kim, "Convolutional neural networks for sentence classification," EMNLP, pp. 1746–1751, 2014.
20. S. Poria, E. Cambria, R. Bajpai, and A. Hussain, "A review of affective computing: From unimodal analysis to multimodal fusion," Information Fusion, vol. 37, pp. 98–125, 2017.
21. A. Zadeh, P. P. Liang, S. Poria, E. Cambria, and L. Morency, "Multimodal language analysis in the wild: CMU-MOSEI dataset and interpretable dynamic fusion graph," ACL, 2018.
22. B. Schuller, S. Steidl, and A. Batliner, "The INTERSPEECH 2013 computational paralinguistics challenge," INTERSPEECH, pp. 148–152, 2013.
23. S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, 1997.
24. D. Hazarika, S. Poria, R. Mihalcea, E. Cambria, and R. Zimmermann, "ICON: Interactive conversational memory network for multimodal emotion detection," EMNLP, 2018.
25. B. Aathavan, "Prevention of ARP spoofing in WLAN," International Journal for Research in Applied Science and Engineering Technology, vol. 13, no. 2, pp. 1–7, 2025