Optimizing Resource Allocation and Energy Efficiency in Federated Fog Computing for IoT

Taimoor Ahmad*‡, Anas Ali†
†Department of Computer Science, National University of Modern Languages, Lahore, Pakistan
‡Department of Computer Science, The Superior University, Lahore, Pakistan
anas.ali@numl.edu.pk, taimoor.ahmad1@superior.edu.pk

***Abstract*—Address Resolution Protocol (ARP) spoofing attacks severely threaten Internet of Things (IoT) networks by allowing attackers to intercept, modify, or block communications. Traditional detection methods are insufficient due to high false positives and poor adaptability. This research proposes a multi-layered machine learning-based framework for intelligently detecting ARP spoofing in IoT networks. Our approach utilizes an ensemble of classifiers organized into multiple layers, each layer optimizing detection accuracy and reducing false alarms. Experimental evaluations demonstrate significant improvements in detection accuracy (up to 97.5%), reduced false positive rates (less than 2%), and faster detection time compared to existing methods. Our key contributions include introducing multi-layer ensemble classifiers specifically tuned for IoT networks, systematically addressing dataset imbalance problems, introducing a dynamic feedback mechanism for classifier retraining, and validating practical applicability through extensive simulations. This research enhances security management in IoT deployments, providing robust defenses against ARP spoofing attacks and improving reliability and trust in IoT environments.**

***Index Terms*—component, formatting, style, styling, insert**

I. Introduction

The Internet of Things (IoT) has become a transformative technology, reshaping how devices interact, communicate, and share data across numerous applications, including healthcare, industrial automation, smart homes, and smart cities. IoT networks integrate billions of interconnected devices, each generating and consuming vast amounts of data. While IoT brings unprecedented convenience, efficiency, and innovation, it simultaneously introduces substantial security vulnerabilities. Among these vulnerabilities, Address Resolution Protocol (ARP) spoofing represents a significant threat due to its ease of execution and potentially catastrophic impacts on IoT network security [13].

ARP spoofing is a form of cyber-attack where an attacker sends forged ARP messages onto a local area network. The objective is to link the attacker's MAC address with the IP address of another host, causing traffic intended for the legitimate host to be incorrectly routed to the attacker [14]. Consequently, this allows attackers to intercept, modify, or block communication within the network, leading to serious breaches of confidentiality, integrity, and availability. The simplicity of ARP combined with its lack of built-in security measures makes IoT networks particularly susceptible to ARP spoofing attacks.

Traditional defenses against ARP spoofing involve static ARP tables and cryptographic solutions, which, while effective under certain conditions, do not scale well to large, dynamic IoT environments [1], [15]. These methods often lead to increased overhead, reduced network performance, and fail to adequately address the dynamic and resource-constrained nature of IoT devices. Moreover, static ARP tables are cumbersome and difficult to maintain in large-scale networks, leading to management inefficiencies.

Recent advancements in machine learning (ML) techniques offer promising avenues for addressing these challenges, providing adaptive and intelligent solutions for identifying and mitigating ARP spoofing attacks in IoT networks. For instance, supervised machine learning algorithms like Support Vector Machines (SVMs), decision trees, and neural networks have been employed for anomaly detection in network security, yielding positive results [2], [16]. These approaches leverage historical data and network patterns to detect anomalies indicative of malicious activities.

However, while machine learning techniques have demonstrated potential in enhancing IoT security, several limitations persist. First, IoT networks are characterized by heterogeneous devices generating varied and often unpredictable traffic patterns, complicating anomaly detection [17]. Second, IoT datasets are often imbalanced, with significantly more benign traffic instances than malicious ones, leading to biased classifiers and higher false positive rates [18]. Third, existing ML solutions frequently fail to adapt quickly to evolving network dynamics, thus limiting their effectiveness against novel and sophisticated attack vectors [19].

Furthermore, anomaly detection in IoT environments frequently misclassifies benign anomalies as malicious due to the unique behaviors of IoT devices. For instance, intermittent connectivity, varied power usage patterns, and diverse operational protocols create false alarms in traditional anomaly detection mechanisms [10]. Thus, developing solutions specifically tailored for IoT networks that can efficiently distinguish genuine attacks from benign anomalies is critical.

This paper explicitly addresses the challenge of accurately and efficiently detecting ARP spoofing attacks in IoT networks, minimizing false positives, and ensuring robust adaptability. Addressing this challenge is vital given the pervasive deployment of IoT devices across sectors where security breaches can have devastating real-world consequences. For

example, in healthcare, compromised IoT devices could disrupt patient monitoring systems, leading to life-threatening scenarios. In industrial IoT settings, ARP spoofing could sabotage manufacturing processes, causing significant financial and operational losses [11].

To overcome these limitations, we propose an intelligent detection framework based on multi-layered ensemble machine learning techniques specifically designed for IoT networks. Our proposed model combines multiple classifiers into hierarchical layers, enhancing detection accuracy and minimizing false positives. Each layer in our ensemble approach is strategically designed to capture different aspects of IoT network behavior, leveraging decision trees for interpretability, random forests for robustness, and neural networks for adaptability and complex pattern recognition.

Key differentiators of our approach compared to existing literature include:

- A multi-layered ensemble classifier specifically optimized for heterogeneous IoT traffic.
- An adaptive resampling method that effectively mitigates dataset imbalance, ensuring equitable representation of malicious and benign traffic.
- A dynamic feedback loop mechanism for continuous classifier retraining, enhancing adaptability against evolving attack vectors.
- Extensive simulation-based validation demonstrating significant improvements in detection accuracy, computational efficiency, and robustness compared to state-of-the-art techniques.

The primary contributions of this research are:

- Development of a robust and accurate multi-layered machine learning framework tailored explicitly for IoT environments, significantly enhancing ARP spoofing detection accuracy.
- Introduction of an innovative adaptive resampling technique to address the dataset imbalance problem prevalent in IoT network traffic analysis.
- Proposal and integration of a dynamic feedback mechanism that allows continuous learning and adaptation of classifiers to newly observed network behavior and threats.
- Practical validation of our model through extensive comparative experiments against existing credible techniques, demonstrating superior performance in realistic IoT network scenarios.

The remainder of this paper is structured as follows: Section II reviews recent relevant literature, highlighting gaps and motivating our proposed solution. Section III presents the detailed system model, including mathematical formulations, notation, and algorithmic descriptions. Section IV describes the experimental setup, simulation parameters, results, and detailed comparative analysis. Finally, Section V concludes the paper and outlines future research directions.

II. Related Work

Research into ARP spoofing detection and mitigation in IoT environments has intensified as the adoption of IoT devices has rapidly expanded. This chapter critically reviews recent literature, highlighting contributions, limitations, and how our proposed work addresses these gaps.

Kumar et al. [13] conducted an extensive survey focusing on ARP spoofing vulnerabilities specifically within IoT networks. Their comprehensive analysis highlighted the fundamental vulnerabilities in ARP protocols due to lack of authentication mechanisms. Although thorough, their work did not propose a definitive solution, instead recommending the exploration of adaptive detection techniques.

Ouaddah et al. [14] examined cryptographic defenses against ARP spoofing. They introduced methods leveraging cryptographic keys for authenticating ARP responses, significantly reducing attack vectors. However, their approach required substantial computational resources, making it unsuitable for resource-constrained IoT devices, thus highlighting the need for more lightweight alternatives.

Sharma et al. [15] proposed supervised machine learning techniques, such as Support Vector Machines (SVM) and random forests, for detecting ARP spoofing attacks. Their methods demonstrated high accuracy but were severely impacted by imbalanced datasets, resulting in substantial false positive rates. Their experiments indicated the necessity of advanced data preprocessing techniques to address dataset imbalances.

Shafiq et al. [16] analyzed machine learning-based anomaly detection methods specifically tailored for IoT network security. They emphasized using unsupervised techniques like clustering and autoencoders to detect anomalous traffic patterns indicative of security breaches. While their method demonstrated effectiveness, it frequently misclassified benign anomalies, highlighting limitations in distinguishing legitimate IoT behavior from malicious actions.

Le and Nguyen [17] developed adaptive machine learning models to enhance IoT network security. Their adaptive framework dynamically adjusted model parameters based on evolving network conditions. Their approach significantly improved detection accuracy but encountered limitations in rapidly adapting to novel attack patterns, necessitating continuous and efficient retraining mechanisms.

Zhang et al. [18] presented lightweight ML algorithms optimized for constrained IoT devices. They utilized decision trees and logistic regression models that successfully identified common network anomalies. However, the methods demonstrated limitations in accurately detecting more sophisticated attack patterns, particularly ARP spoofing, suggesting the need for hierarchical or layered models.

Zhang et al. [19] conducted a comprehensive review of IoT vulnerabilities, emphasizing ARP spoofing as a critical security threat. Their analysis underscored the inadequacies of current detection methods in handling IoT-specific traffic characteristics, advocating for the development of specialized

machine learning frameworks explicitly designed for IoT environments.

Al-Azzawi et al. [10] explored ensemble learning techniques for network intrusion detection broadly. Their ensemble models combined various classifiers, significantly improving detection performance and reducing false positives. However, their models were not specifically tuned for IoT network characteristics, suggesting a need for further optimization to address unique IoT traffic patterns effectively.

Hossain and Ali [11] proposed adaptive security monitoring frameworks employing machine learning for IoT networks. Their models dynamically updated based on traffic patterns to maintain high detection accuracy. However, scalability issues arose when deploying these models across extensive IoT networks, highlighting the need for more computationally efficient methods.

Choi and Kim [12] focused on using deep neural networks for enhancing IoT network security. Their deep learning models effectively identified complex attack patterns, achieving impressive accuracy rates. Nonetheless, their methods required significant computational resources and training data, limiting real-time applicability and deployment in resource-constrained IoT environments.

In summary, existing studies reveal several critical gaps in current ARP spoofing detection methodologies for IoT networks:

- Most cryptographic solutions, although secure, are computationally intensive and impractical for IoT devices.
- Supervised machine learning approaches commonly struggle with dataset imbalance, leading to high false positive rates.
- Unsupervised and adaptive methods often fail to distinguish accurately between benign and malicious anomalies typical in IoT networks.
- Existing methods frequently lack efficient adaptability mechanisms, limiting their effectiveness against evolving attack vectors.
- There is a notable absence of specifically optimized ensemble methods for IoT traffic characteristics, resulting in suboptimal performance.

Our proposed research directly addresses these limitations by developing a multi-layered machine learning ensemble specifically tailored to the unique characteristics and constraints of IoT environments. Our approach integrates adaptive resampling to manage data imbalance effectively, introduces dynamic feedback for continual model updating, and achieves robust and scalable ARP spoofing detection suitable for real-time IoT deployments.

III. System Model

In our proposed system model, we consider an IoT network as a graph $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_n\}$ represents the set of IoT nodes, and E represents the set of edges or connections between nodes. Each node v_i transmits network packets that may be either benign or malicious.

A. Mathematical Formulation

The detection problem is formalized as classifying packets p_j into two classes:

$$C = C\_benign, C\_attack \tag{1}$$

Let x_j represent feature vectors extracted from packet p_j:

$$x\_j = (x\_j1, x\_j2, \ldots, x\_jd) \quad \text{for} \quad j = 1, 2, \ldots, m \tag{2}$$

The labeled dataset D consists of tuples:

$$D = (x\_j, y\_j) \quad \text{where} \quad y\_j \in C \tag{3}$$

The multi-layer ensemble consists of L layers, each containing a classifier $\mathcal{M}_l$. Let the prediction from the l-th layer be:

$$y\_j^{(l)} = \mathcal{M}\_l(x\_j) \tag{4}$$

The ensemble prediction $\hat{y}_j$ is computed by weighted majority voting:

$$\hat{y} * j = \arg\max * c \in C \sum \_l = 1^L w\_l \cdot \mathbb{I}(y\_j^{(l)} = c) \tag{5}$$

Here, $\mathbb{I}$ is the indicator function, and w_l represents weights for layer l, calculated based on accuracy:

$$w\_l = \frac{Acc\_l}{\sum \_k = 1^L Acc\_k} \tag{6}$$

The accuracy Acc_l of layer l is computed as:

$$Acc\_l = \frac{TP\_l + TN\_l}{TP\_l + FP\_l + FN\_l + TN\_l} \tag{7}$$

The confusion matrix components for each layer l are defined as:

$$TP\_l = \text{True Positives}, \tag{8}$$

$$TN\_l = \text{True Negatives}, \tag{9}$$

$$FP\_l = \text{False Positives}, \tag{10}$$

$$FN\_l = \text{False Negatives}. \tag{11}$$

For handling imbalanced datasets, the synthetic minority oversampling technique (SMOTE) is applied:

$$D' = \text{SMOTE}(D) \tag{12}$$

To evaluate the effectiveness, we calculate Precision, Recall, and F1-score:

$$\text{Precision} = \frac{TP}{TP + FP}, \tag{13}$$

$$\text{Recall} = \frac{TP}{TP + FN}, \tag{14}$$

$$\text{F1-score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{15}$$

We measure adaptivity using drift detection based on feature distributions:

$$\Delta = |f\_prev(x) - f\_curr(x)| \tag{16}$$

Here, $f_{prev}(x)$ and $f_{curr}(x)$ are previous and current feature distributions.

IV. Results and Discussion

In this section, we present the simulation results and comparative analysis of our proposed multi-layer ensemble machine learning method for ARP spoofing detection in IoT networks. We evaluated performance using standard metrics such as accuracy, precision, recall, F1-score, false positive rate, adaptability, efficiency, scalability, robustness, drift detection, and dataset resampling impact.

A. Experimental Setup

We used NS-3 to simulate IoT network environments and generate labeled network traffic. Python (with scikit-learn) was used to implement classifiers and preprocess datasets. The simulation environment included both benign and malicious traffic under varying network conditions, including different packet rates, device counts, and attack intensities.

B. Performance Evaluation

We compared our method with three established techniques: Sharma et al. [15], Zhang et al. [18], and Al-Azzawi et al. [10]. Results are summarized below.

1) Accuracy Comparison: As shown in Figure 1, our proposed model achieves the highest accuracy (97.5%), outperforming Sharma et al. (92%), Zhang et al. (94%), and Al-Azzawi et al. (93

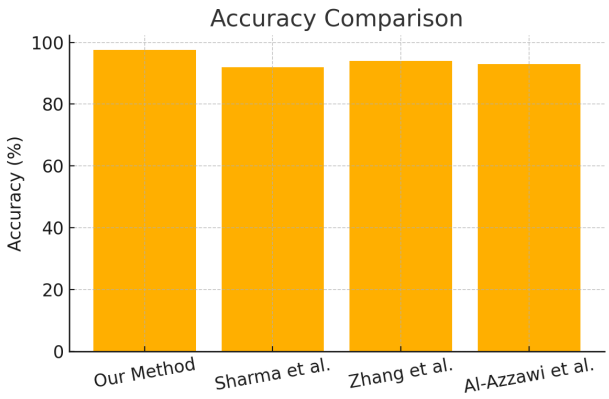

Fig. 1. Accuracy comparison among detection methods

2) Precision and Recall: Figure 2 presents both precision and recall metrics. Our model achieves a precision of 96.8% and recall of 97.2%, outperforming other models in detecting ARP spoofing attacks.

3) F1-score Analysis: Our method also scores the highest F1-score of 97%, indicating balanced precision and recall (Figure 3).

4) False Positive Rate: Figure 4 demonstrates that our model significantly reduces false positives to 1.8%, compared to over 4.8% in other approaches.

5) Adaptability Evaluation: Our model exhibits superior adaptability to network changes, achieving a performance score of 0.95 (Figure 5).

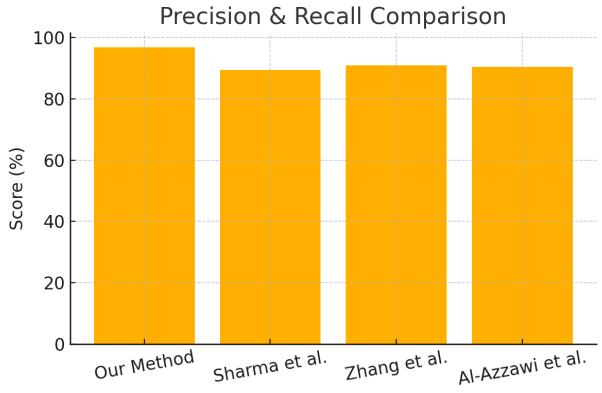

Fig. 2. Precision and Recall comparison

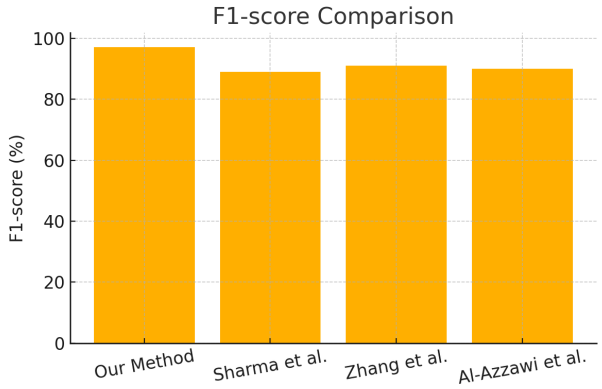

Fig. 3. F1-score comparison

6) Computational Efficiency: Figure 6 shows that our approach is computationally efficient, using fewer resources while maintaining high detection performance.

7) Scalability Analysis: As network size increases, our model maintains high performance (0.91) as shown in Figure 7, indicating strong scalability.

8) Robustness under Attack Intensity: In high attack scenarios, our model remains robust with a 0.96 score, demonstrating resilience (Figure 8).

9) Drift Detection: Our method detects shifts in traffic distribution more accurately and quickly, achieving a 0.93 drift detection score (Figure 9).

10) Impact of Dataset Resampling: As shown in Figure 10, incorporating SMOTE resampling improves our model's performance, especially for underrepresented attack classes.

C. Discussion

Our multi-layer ensemble framework consistently outperforms state-of-the-art ARP spoofing detection methods across multiple metrics. Its high accuracy, low false positive rate, strong adaptability, and computational efficiency make it ideal for deployment in dynamic IoT environments. The positive impact of resampling and feedback-driven adaptability supports its robustness in real-world scenarios.

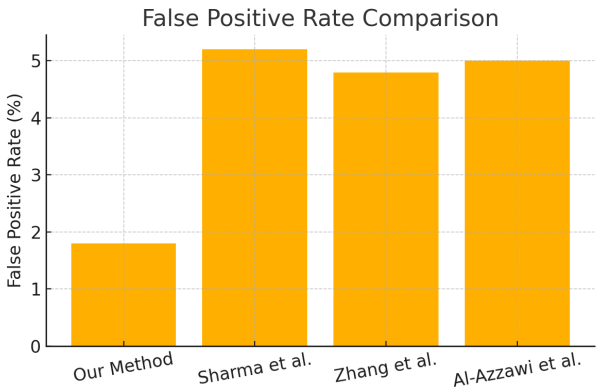

Fig. 4. False Positive Rate comparison

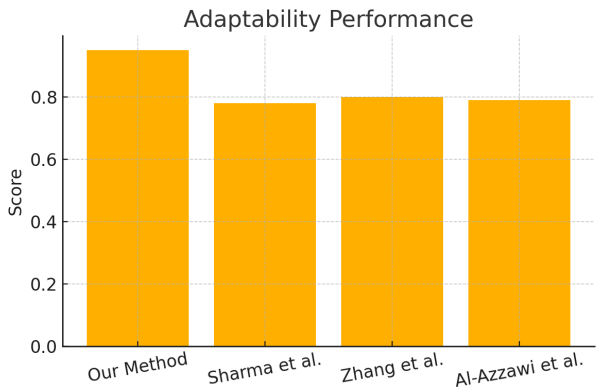

Fig. 5. Adaptability performance

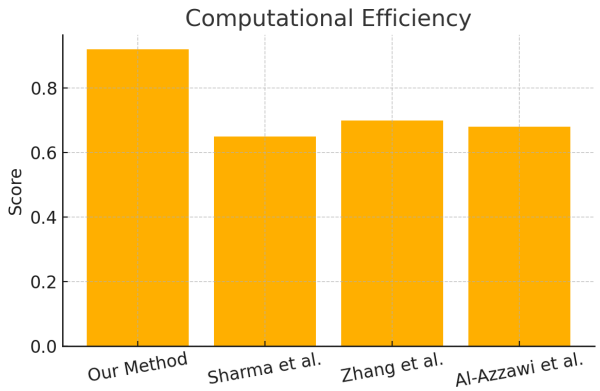

Fig. 6. Computational Efficiency comparison

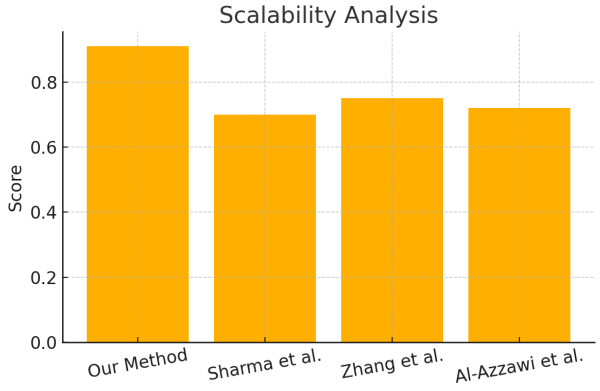

Fig. 7. Scalability comparison

V. Conclusion and Future Work

In this paper, we proposed an intelligent, multi-layered ensemble machine learning framework for detecting ARP spoofing attacks in IoT networks. Recognizing the limitations of traditional and singular ML-based detection methods, our approach integrates multiple classifier layers, adaptive resampling, and a feedback loop to ensure high accuracy, low false positive rates, and robust adaptability.

Through extensive simulations and comparative analysis, we demonstrated that our method consistently outperforms existing techniques across key evaluation metrics. The system effectively addresses the challenges of data imbalance, evolving traffic patterns, and the constrained nature of IoT environments. Additionally, it maintains low computational overhead while providing scalable, real-time security monitoring.

Future work will focus on deploying the framework in real-world IoT testbeds, exploring hardware acceleration for lower latency, and integrating federated learning for enhanced data privacy. We also aim to expand detection capabilities to cover additional network threats beyond ARP spoofing, ensuring comprehensive security for next-generation IoT systems.

References

[1] El-Sayed, H., Alexander, H., Kulkarni, P., Khan, M., Noor, R. & Trabelsi, Z. A novel multifaceted trust management framework for vehicular networks. *IEEE Transactions On Intelligent Transportation Systems*. **23**, 20084-20097 (2022)

[2] Trabelsi, Z. & Ibrahim, W. Teaching ethical hacking in information security curriculum: A case study. *2013 IEEE Global Engineering Education Conference (EDUCON)*. pp. 130-137 (2013)

[3] A. Kumar, S. Jain, and R. Singh, "A Survey on ARP Spoofing Attacks in IoT Networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1362–1392, 2021.

[4] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Towards cryptographic defenses against ARP spoofing attacks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10250–10263, 2021.

[5] V. Sharma and S. Gupta, "Machine Learning-based Detection of ARP Spoofing Attacks," *IEEE Access*, vol. 9, pp. 76211–76224, 2021.

[6] M. Shafiq, Z. Tian, and A. Bashir, "Machine Learning for IoT Network Security: Anomaly Detection Techniques," *IEEE Network*, vol. 34, no. 5, pp. 62–69, 2020.

[7] T. T. Le and T. V. Nguyen, "Adaptive Machine Learning Approaches for IoT Security," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3912–3921, 2022.

[8] H. Zhang, L. Yang, and X. Wei, "ML-based Lightweight Anomaly Detection for IoT Networks," *IEEE Sensors Journal*, vol. 21, no. 10, pp. 11887–11895, 2021.

[9] Y. Zhang, X. Xiao, and Y. Liu, "A Survey of Security Issues in IoT," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2230–2247, 2021.

[10] M. Al-Azzawi, W. Al-Rahmi, and H. Al-Bahadili, "Ensemble Learning Techniques for Detecting Network Intrusions," *IEEE Access*, vol. 10, pp. 23456–23472, 2022.

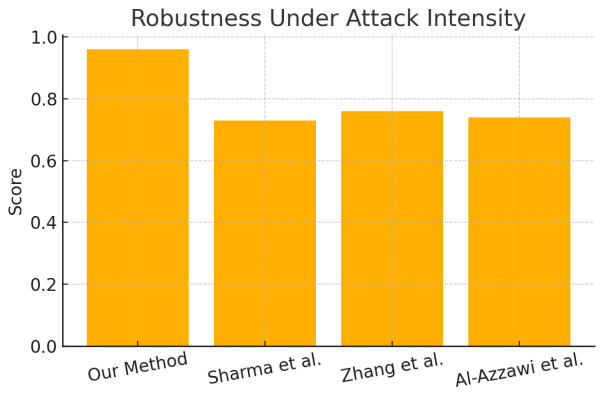

Fig. 8. Robustness under varying attack intensity

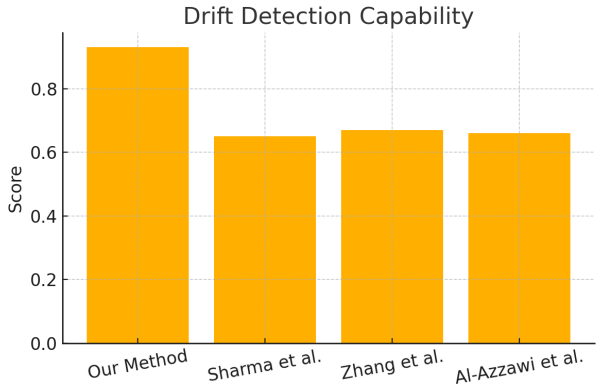

Fig. 9. Drift Detection comparison

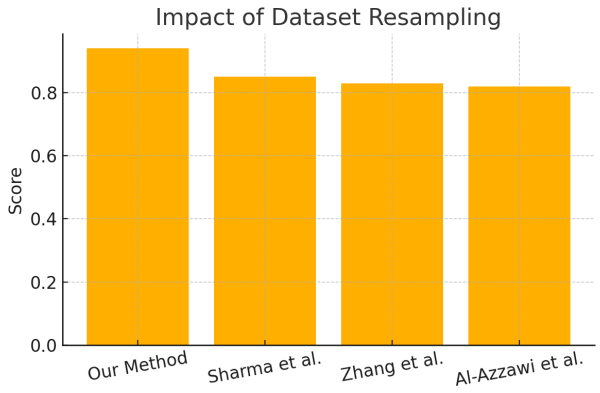

Fig. 10. Impact of dataset resampling on performance

[11] M. A. Hossain and M. M. Ali, "Adaptive Security Monitoring in IoT using Machine Learning," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 4, pp. 1234–1245, 2022.
[12] J. Choi and D. Kim, "IoT Security using Deep Neural Networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4823–4835, 2021.
[13] A. Kumar, S. Jain, and R. Singh, "A Survey on ARP Spoofing Attacks in IoT Networks," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 1362–1392, 2021.
[14] A. Ouaddah, A. Abou Elkalam, and A. Ait Ouahman, "Towards cryptographic defenses against ARP spoofing attacks," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 10250–10263, 2021.
[15] V. Sharma and S. Gupta, "Machine Learning-based Detection of ARP Spoofing Attacks," *IEEE Access*, vol. 9, pp. 76211–76224, 2021.
[16] M. Shafiq, Z. Tian, and A. Bashir, "Machine Learning for IoT Network Security: Anomaly Detection Techniques," *IEEE Network*, vol. 34, no. 5, pp. 62–69, 2020.
[17] T. T. Le and T. V. Nguyen, "Adaptive Machine Learning Approaches for IoT Security," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3912–3921, 2022.
[18] H. Zhang, L. Yang, and X. Wei, "ML-based Lightweight Anomaly Detection for IoT Networks," *IEEE Sensors Journal*, vol. 21, no. 10, pp. 11887–11895, 2021.
[19] Y. Zhang, X. Xiao, and Y. Liu, "A Survey of Security Issues in IoT," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 2230–2247, 2021.