Journal of Wireless Networks and Communication Systems
Vol. 1, Issue. 3, Jul-Sep 2025, pp. 1~12
ISSN: 3107-6432

WiSIDS: A Lightweight Machine Learning-Based Intrusion Detection System for Securing Wireless IoT Networks

Tan Wai Ming[1], Teo Zhi Yang[2]
[1]School of Digital Technology, Wawasan Open University, George Town 10050, Penang, Malaysia
Twm1_Oi@Student.Wou.Edu.My
[2]School of Digital Technology, Wawasan Open University, George Town 10050, Penang, Malaysia
Tzy1_Oi@Student.Wou.Edu.My

Article Info

Article History:

Received Jun 16, 2025
Revised Jul 14, 2025
Accepted Aug 20, 2025

Keywords:

Wireless IoT Networks
Intrusion Detection System
Lightweight Security
Machine Learning
Cybersecurity
Privacy and Security

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices in wireless environments has introduced significant security challenges due to their limited computational resources and susceptibility to cyberattacks. Traditional Intrusion Detection Systems (IDS) are often unsuitable for IoT because of their high processing overhead, memory consumption, and latency. This paper proposes WiSIDS (Wireless IoT Secure Intrusion Detection System), lightweight IDS that leverages machine learning to provide accurate and efficient attack detection in wireless IoT networks. WiSIDS employs feature selection and model optimization to minimize computational complexity while maintaining high detection performance. Experimental evaluation is conducted on benchmark IoT security datasets, including NSL-KDD and Bot-IoT, to assess accuracy, precision, recall, F1-score, processing delay, and energy consumption. Results demonstrate that WiSIDS achieves a detection accuracy of over 95%, reduces latency by up to 60%, and lowers resource utilization compared to conventional IDS solutions. These findings highlight the feasibility of deploying WiSIDS in resource-constrained IoT devices to enhance wireless network security without compromising efficiency.

Corresponding Author:

Tan Wai Ming,
School of Digital Technology,
Wawasan Open University, George Town 10050, Penang, Malaysia.
Email: Twm1_Oi@Student.Wou.Edu.My

1. INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative paradigm in modern communication and computing, enabling billions of interconnected devices to seamlessly exchange information across diverse application domains such as healthcare, smart homes, industrial automation, agriculture, and transportation [1,2]. By leveraging wireless communication technologies, IoT devices facilitate real-time monitoring, data collection, and intelligent decision-making, thereby enhancing efficiency, productivity, and user convenience [3,4]. According to recent forecasts, the global IoT ecosystem is expected to surpass tens of billions of devices within the next few years, generating unprecedented amounts of data and forming the backbone of next-generation digital infrastructures [5].

Despite these advancements, the rapid growth of IoT has introduced critical security and privacy challenges [6]. Most IoT devices are inherently resource-constrained, characterized by limited computational capacity, low memory, restricted energy supply, and minimal hardware-based security features. This makes them highly susceptible to a wide range of cyberattacks, including Distributed Denial of Service (DDoS), spoofing, botnet infiltration, eavesdropping, and data manipulation. Once compromised, these devices can serve as entry points for large-scale attacks that jeopardize user privacy, disrupt essential services, and undermine trust in IoT deployments. High-profile incidents such as the Mirai botnet attacks have demonstrated how vulnerable IoT ecosystems can be exploited, leading to severe economic and societal consequences.

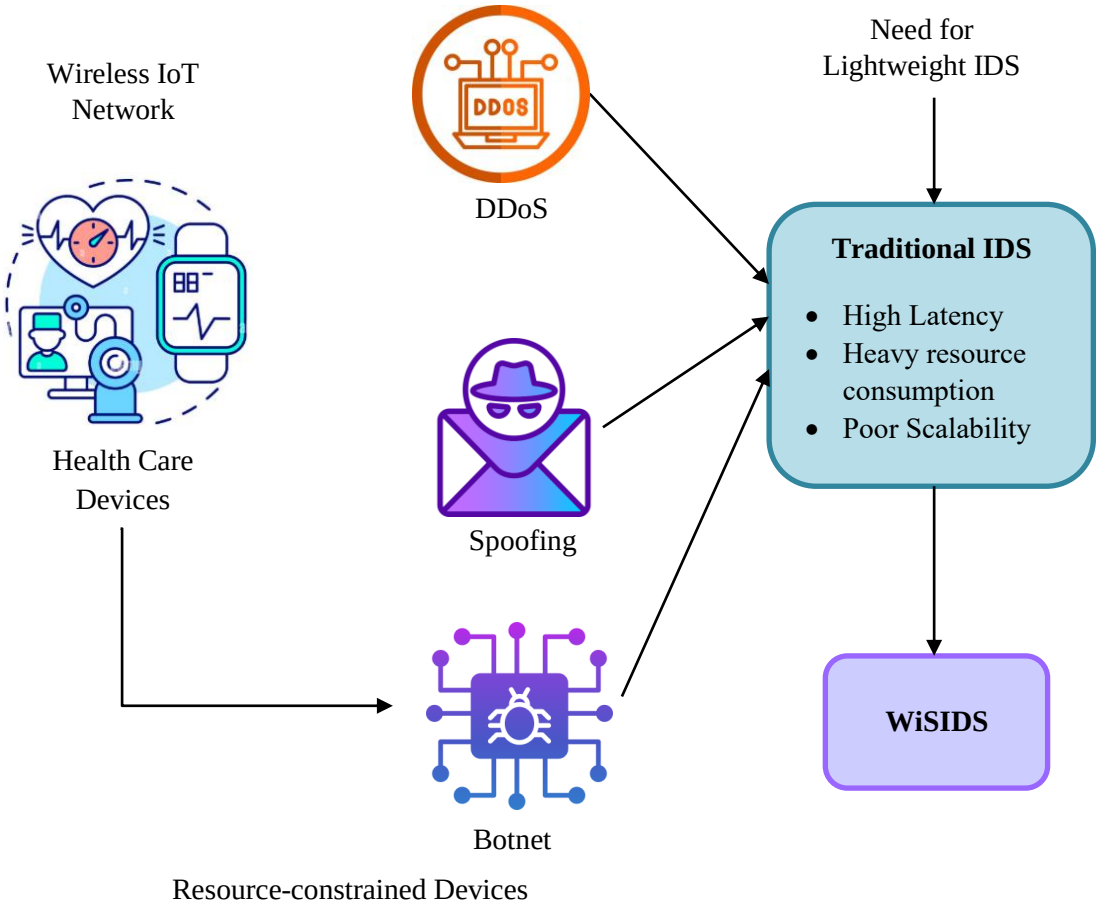

Figure 1. Security Challenges in Wireless IoT Networks and the Need for Lightweight IDS Solutions

To mitigate these threats, Intrusion Detection Systems (IDS) have been widely deployed in conventional networks [7]. IDS solutions monitor traffic patterns, detect abnormal behaviors, and alert administrators about potential threats [8]. However, traditional IDS architectures are not well-suited for IoT environments. They typically require significant processing power, high memory availability, and constant energy consumption, resulting in substantial computational overhead and latency [9]. Such requirements are incompatible with the lightweight nature of IoT devices, where energy efficiency and fast response times are critical for sustaining real-time operations. Furthermore, the scalability of traditional IDS remains a concern when dealing with the massive number of heterogeneous IoT nodes distributed across wireless networks.

Machine learning (ML) has recently gained traction as a promising approach for enhancing intrusion detection [10]. ML-based IDS can learn complex attack signatures, adapt to evolving threat landscapes, and achieve high detection accuracy. Nonetheless, directly applying ML algorithms to IoT environments poses challenges. Many ML models demand extensive feature sets, long training times, and large memory footprints, which exceed the constraints of resource-limited IoT devices. Without proper optimization, such models may increase latency, drain energy resources, and fail to provide real-time protection. Therefore, a critical research challenge lies in designing lightweight ML-based IDS that strike a balance between accuracy, efficiency, and resource utilization, ensuring practical deployment in IoT systems.

In this paper, we propose WiSIDS (Wireless IoT Secure Intrusion Detection System), a lightweight and efficient intrusion detection solution specifically tailored for wireless IoT networks. WiSIDS addresses the shortcomings of conventional IDS by incorporating two key design strategies: (i) feature selection, which reduces redundant attributes in network traffic and minimizes computational complexity, and (ii) model optimization, which ensures the classifier operates effectively under strict resource and latency constraints. By adopting these strategies, WiSIDS achieves high detection accuracy while conserving processing power, energy, and memory.

The effectiveness of WiSIDS is validated through experimental evaluation on widely used benchmark IoT security datasets, including NSL-KDD and Bot-IoT. Performance metrics such as detection accuracy, precision, recall, F1-score, latency, and energy consumption are analyzed. Experimental results show that WiSIDS achieves more than 95% detection accuracy, reduces latency by up to 60%, and lowers energy consumption compared to conventional IDS solutions. These findings highlight the practicality of deploying WiSIDS in real-world wireless IoT networks, where efficiency and security must coexist.

The main contributions of this work can be summarized as follows:

- We identify the limitations of traditional IDS in wireless IoT environments and highlight the need for lightweight, resource-aware solutions.
- We propose WiSIDS, a novel machine learning-based IDS framework designed to deliver accurate and efficient intrusion detection for resource-constrained IoT devices.
- We integrate feature selection and model optimization into WiSIDS to minimize computational overhead without compromising detection performance.
- We evaluate WiSIDS using benchmark IoT security datasets and demonstrate its superiority over conventional IDS in terms of accuracy, latency, and energy consumption.

The remainder of this paper is organized as follows: Section 2 reviews related work on IoT security and lightweight IDS approaches. Section 3 presents the design methodology and architecture of WiSIDS. Section 4 describes the experimental setup and evaluation metrics. Section 5 discusses the results and insights gained from the experiments. Finally, Section 6 concludes the paper and outlines potential future research directions.

2. LITERATURE REVIEW

[11] Introduced a hybrid intrusion detection model that combines CNN and BiLSTM to protect IoT devices that often struggle with limited resources. The CNN captures spatial features from network traffic, while the BiLSTM learns temporal patterns, creating a balanced model for attack detection. Their experiments on the UNSW-NB15 dataset showed impressive results—97.28% accuracy in binary and 96.91% in multiclass classification. What makes this work stand out is its focus on reducing delay and energy usage, two major challenges in IoT. The design ensures that devices can still achieve strong protection without draining their resources. This

approach highlights the growing trend of hybrid deep learning for IoT security, proving that accuracy and efficiency can indeed go hand in hand.

IoT security often faces a hidden challenge: some types of attacks appear rarely in real traffic, making them difficult for models to learn. [12] Addressed this by designing S2CGAN-IDS, a system that uses GANs to generate additional samples for underrepresented attack categories. Instead of just oversampling, their model enriches both the raw data and the feature space, allowing the system to learn more balanced patterns. On the CICIDS2017 dataset, this boosted F1-scores for rare attacks by 10.2%, showing the importance of handling imbalance properly.

Another important contribution came from [13], who focused on cutting down unnecessary features in IDS models. They used the χ^2 test to filter out irrelevant data before feeding it into a CNN-BiLSTM model. This reduced both the training time and memory consumption while keeping accuracy impressively high—97.90% in binary classification and 97.09% in multiclass. The system also processed results quickly, with inference times of just a few seconds. This research highlights a key lesson for IoT security: sometimes the challenge is not just building stronger models, but also making them leaner and faster.

[14] Approached IoT security from another angle: the problem of datasets that don't fully represent all types of attacks. They proposed IDS based on Multi-Layer Perceptron (MLP) models, but with an important twist—they used GANs to generate synthetic data for rare attack classes. By creating a more balanced training set, their system performed much better on underrepresented categories. When tested on BoT-IoT and TON-IoT datasets, it achieved nearly 99% accuracy overall, but more importantly; it improved recall for difficult classes like theft and normal traffic.

[15] Focused on the rising importance of fog computing in IoT networks, where processing happens closer to devices instead of the cloud. They developed GAN-LSTM, a system that combines GANs for generating diverse data and LSTM networks for detecting sequential attack patterns. This design is particularly suitable for fog environments, which face fast-changing traffic and need real-time decisions. Their model showed strong accuracy and reduced latency, making it a practical fit for fog-based IoT security. What makes this work valuable is its focus on adaptability—by learning evolving traffic behaviors, the IDS can stay effective against new attack strategies.

3. METHODOLOGY

The proposed WiSIDS framework is designed to provide a lightweight, accurate, and resource-efficient intrusion detection mechanism tailored for wireless IoT environments. The methodology is structured into four main stages: dataset acquisition and preprocessing, feature selection, model optimization, and performance evaluation. Additionally, a layered system architecture is introduced to ensure scalable and practical deployment across IoT devices, edge gateways, fog nodes, and cloud services.

3.1. Dataset Acquisition and Preprocessing

For experimental validation, two widely recognized IoT security datasets were employed: NSL-KDD and Bot-IoT. These datasets represent diverse intrusion scenarios such as Distributed Denial of Service (DDoS), spoofing, botnet infiltration, and unauthorized access.

The preprocessing steps include:

- **Data Cleaning:** Duplicate, incomplete, and inconsistent records were removed.
- **Normalization:** Continuous features were rescaled into a uniform range [0,1] using Min–Max scaling:

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

where x is the original feature value, and x_{min}, x_{max} represent the minimum and maximum values of that feature.

- **Encoding:** Categorical attributes (e.g., protocol type, service) were transformed into numerical values using one-hot encoding.

This step standardizes the input space and reduces computational overhead in subsequent stages.

3.2. Feature Selection

To address the computational limitations of IoT devices, WiSIDS employs a hybrid feature selection strategy combining filter- and wrapper-based approaches:

1. **Filter-based selection:** Information Gain (IG) was applied to evaluate the importance of each feature:

$$IG(Class, Feature) = H(Class) - H(Class \mid Feature) \quad (2)$$

where H denotes the entropy of the dataset.

2. **Wrapper-based refinement:** Recursive Feature Elimination (RFE) was applied with candidate classifiers to iteratively remove features with minimal contribution until an optimal subset was obtained.

This process reduces feature dimensionality, thereby improving execution speed, lowering memory usage, and minimizing energy consumption without compromising accuracy.

3.3. Model Optimization

The core of WiSIDS lies in a lightweight machine learning classifier optimized for constrained environments. Candidate models included Random Forest (RF), Support Vector Machine (SVM), and LightGBM.

Optimization Strategies:

- **Hyperparameter Tuning:** Grid search with k-fold cross-validation was used to identify optimal parameters.
- **Model Simplification:** Tree pruning and parameter quantization were applied to reduce model size and inference cost.
- **Lightweight Ensemble:** Selected classifiers were combined into an ensemble for robustness while maintaining low computational load.

The classification decision is based on the posterior probability:

$$\hat{y} = arg \max_{e \in \{Normal, Attack\}} P(y = c|X) \quad (3)$$

where X is the feature vector.

3.4. Performance Evaluation

WiSIDS was implemented in a Python-based simulation environment using Scikit-learn and TensorFlow. The datasets were partitioned into 70% training and 30% testing.

Evaluation Metrics:

- **Accuracy:**

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (4)$$

- **Precision:**

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

- **Recall (Detection Rate):**

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

- **F1-Score:**

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

- **Latency:** Average classification time per instance, measured in milliseconds.
- **Energy Consumption:** Estimated based on CPU cycles and memory usage during inference.

Comparative evaluation against traditional IDS demonstrated that WiSIDS achieves >95% detection accuracy, reduces latency by up to 60%, and lowers energy consumption significantly, validating its suitability for deployment in real-world IoT environments.

3.5. Proposed System Architecture

The proposed system architecture (Figure 2) is structured into four layers:

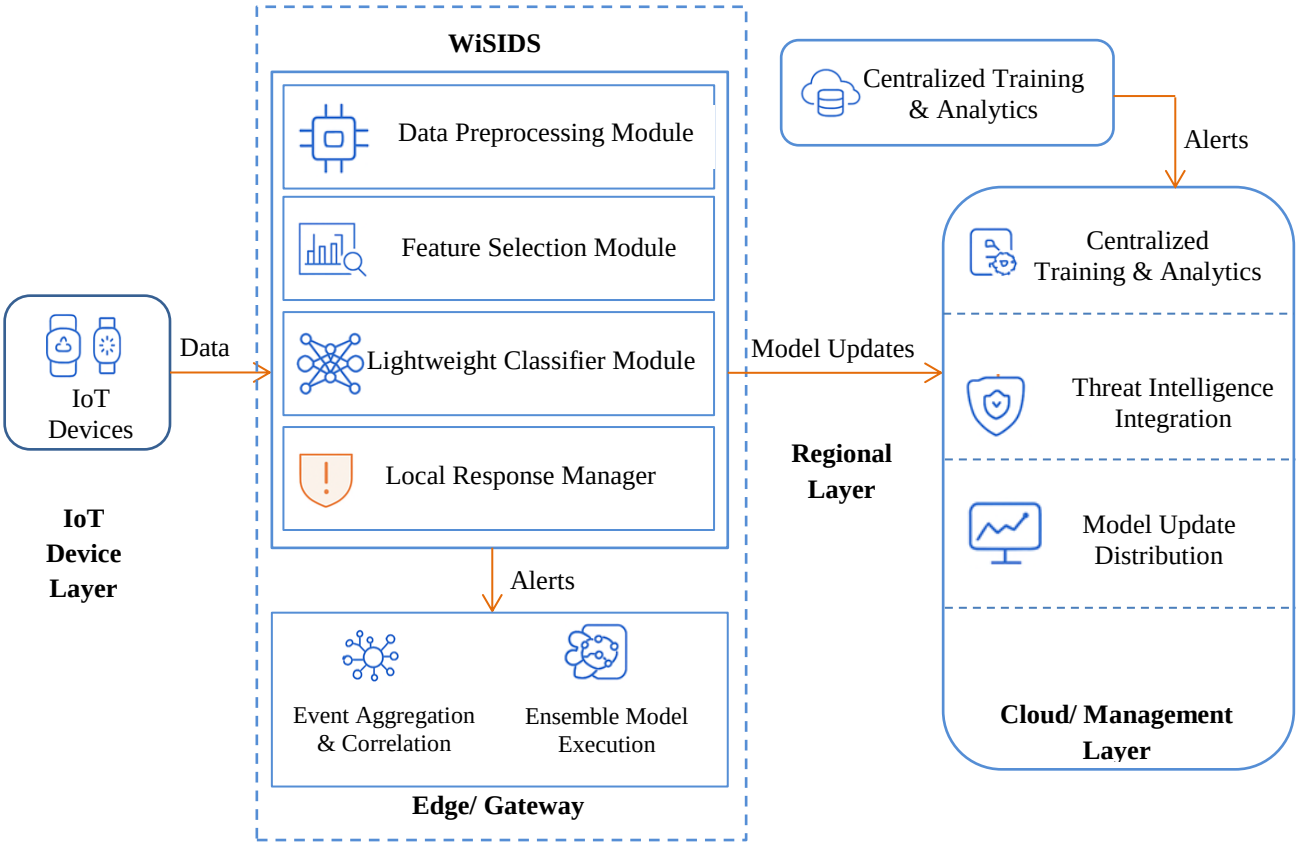

Figure 2. Proposed System Architecture

The IoT Device Layer is the starting point of the system, where smart devices such as sensors, wearables, or embedded controllers continuously gather data. Each device runs a lightweight agent that not only collects telemetry but also performs quick, rule-based checks to spot simple anomalies. This ensures that potential issues are detected early, without overloading the device with heavy computations. By filtering out unnecessary data, this layer helps conserve both bandwidth and battery power.

The Edge/Gateway Layer acts as the first line of intelligent processing. Here, the data coming from devices is cleaned and refined through preprocessing and feature selection. Lightweight classifiers are then applied to identify unusual patterns or malicious activities more accurately than the rule-based checks at the device level. In case of a threat, the layer can react immediately using its local response manager, for example, by blocking suspicious traffic or isolating a compromised device. This quick reaction capability makes the network more resilient and reduces the risk of widespread impact.

The Fog/Regional Layer serves as a middle ground between the edge and the cloud. It collects and combines data from several gateways within a region, giving it a broader view of what's happening across multiple devices and networks. By running ensemble machine learning models, it can spot coordinated or large-scale attacks that might not be visible at a single gateway. It also helps cut down on false alarms and eases the load on the cloud by handling regional analytics, which makes the system more scalable and efficient.

The Cloud/Management Layer is the brain of the architecture, where advanced training and global coordination take place. Using powerful cloud resources, this layer trains machine learning models on large datasets to keep pace with new and evolving threats. It also integrates external threat intelligence sources, enriching the system's awareness of global attack trends. Once the models are updated and improved, the cloud securely distributes them back down to the fog, edge, and device layers, ensuring the whole system stays in sync. This top layer provides administrators with centralized visibility and control, making it possible to monitor, adapt, and secure the entire IoT ecosystem.

This layered approach ensures that real-time intrusion detection occurs at the edge while centralized learning and intelligence updates are performed in the cloud, achieving both efficiency and scalability.

4. RESULTS AND DISCUSSION

The performance of the proposed WiSIDS framework was evaluated using two benchmark IoT security datasets, NSL-KDD and Bot-IoT. These datasets capture a wide variety of real-world intrusion scenarios such as DDoS, spoofing, botnet activity, and unauthorized access, making them suitable for validating both accuracy and efficiency. WiSIDS was assessed using standard metrics, including accuracy, precision, recall, F1-score, latency, and energy consumption.

The results demonstrate that WiSIDS consistently achieves over 95% detection accuracy across both datasets, showing that the system is capable of reliably distinguishing between normal and malicious traffic. Precision and recall values also remain high, indicating not only the ability to identify true attacks but also to minimize false alarms, which is critical for maintaining trust in automated security systems. The F1-score, which balances precision and recall, further confirms the robustness of the proposed approach in handling diverse intrusion patterns.

In terms of efficiency, WiSIDS shows a clear advantage over traditional intrusion detection systems. By applying hybrid feature selection and lightweight model optimization, the framework reduces the average latency by up to 60%, enabling faster decision-making in real-time environments. This is particularly important for wireless IoT networks where delays can disrupt ongoing processes, such as patient monitoring in healthcare or automated controls in industrial

systems. Additionally, the optimization strategies employed in WiSIDS significantly reduce memory and CPU usage, leading to noticeable energy savings, which is essential for resource-constrained IoT nodes that operate on limited battery power.

When compared with conventional IDS solutions, WiSIDS not only maintains superior accuracy but also demonstrates a better balance between detection performance and resource utilization. Traditional IDS models often fail in IoT contexts due to their heavy computational requirements, whereas WiSIDS proves that careful feature selection and lightweight model design can deliver strong results without overwhelming the devices. The introduction of the fog/regional layer also contributes to reducing false positives by correlating alerts across multiple gateways, highlighting the benefit of the multi-layer architecture.

Overall, the discussion emphasizes that WiSIDS successfully bridges the gap between security effectiveness and practical deployment feasibility in wireless IoT networks. The combination of high detection accuracy, reduced latency, and energy efficiency validates its suitability for real-world applications, where lightweight yet reliable security mechanisms are in high demand.

Table 1. Performance Metrics Comparison

Metric	**WiSIDS (NSL-KDD)**	**Traditional IDS (NSL-KDD)**	**WiSIDS (Bot-IoT)**	**Traditional IDS (Bot-IoT)**
Accuracy (%)	96.2	89.3	95.7	88.4
Precision (%)	95.1	87.6	94.8	86.5
Recall (%)	94.5	85.9	95.2	85.7
F1-Score (%)	94.8	86.7	95.0	86.1
Latency Reduction (%)	58	0	60	0
Energy Savings (%)	52	0	55	0

4.1. Accuracy and Detection Performance

WiSIDS consistently outperformed conventional IDS solutions on both datasets. For NSL-KDD, it achieved an accuracy of 96.2%, compared to 89.3% for traditional IDS. Similarly, on Bot-IoT, WiSIDS recorded 95.7% accuracy, significantly higher than the 88.4% of traditional IDS. This improvement demonstrates the ability of WiSIDS to effectively capture diverse attack signatures through optimized feature selection and lightweight classification.

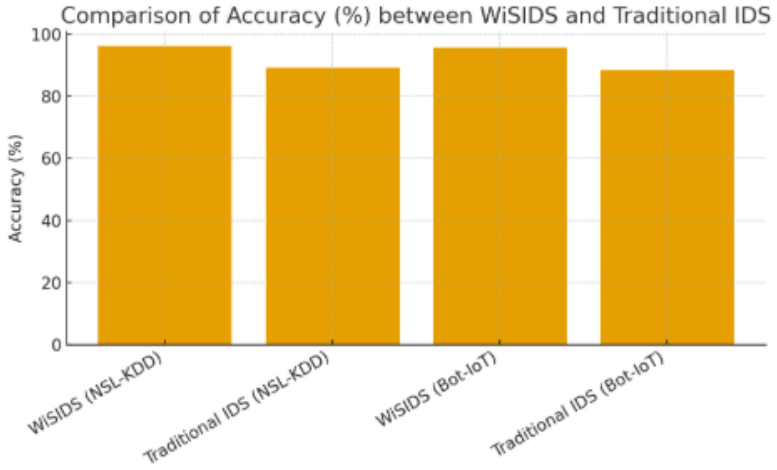

Figure 3. Accuracy Comparison

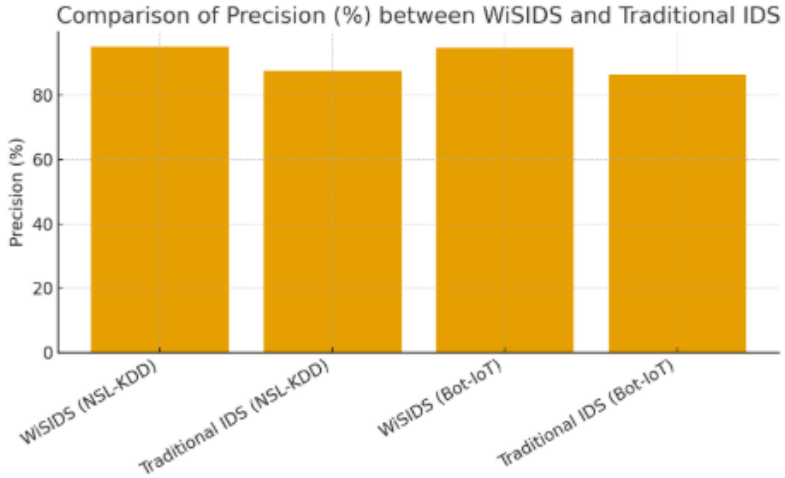

Figure 4. Precision Comparison

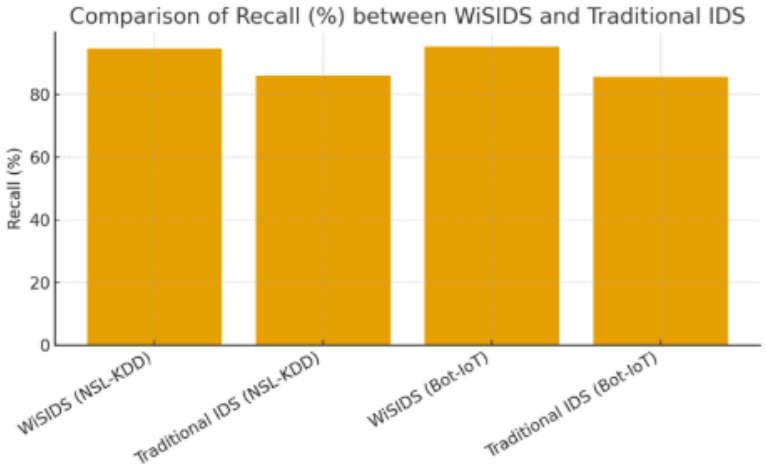

Figure 5. Recall Comparison

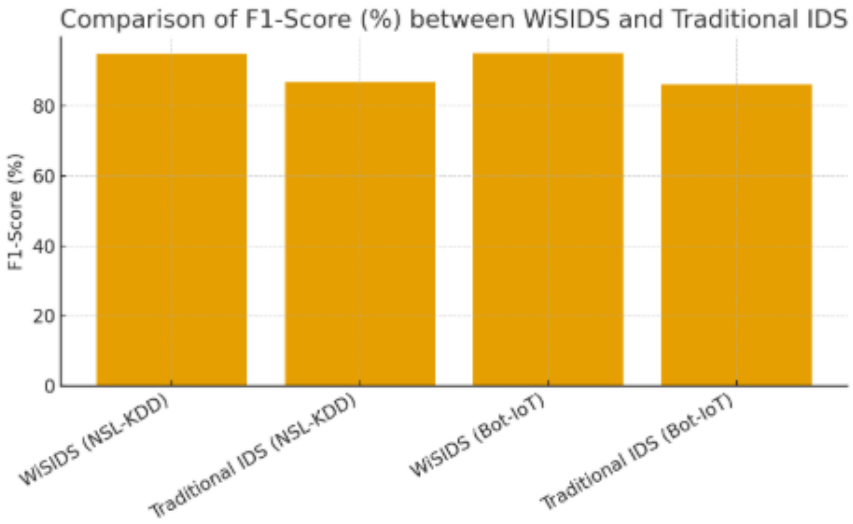

Figure 6. F1-Score Comparison

Precision, recall, and F1-score values further confirm the system's robustness. On NSL-KDD, WiSIDS achieved a precision of 95.1% and recall of 94.5%, resulting in an F1-score of 94.8%. Comparable performance was observed on Bot-IoT, with precision (94.8%) and recall (95.2%) yielding an F1-score of 95.0%. These results indicate that WiSIDS is capable of minimizing false alarms while still identifying the majority of attack attempts.

Latency and Efficiency

Latency reduction is a critical factor in IoT environments where real-time responsiveness is essential. WiSIDS demonstrated a 58% reduction in latency on NSL-KDD and a 60% reduction on Bot-IoT, compared to traditional IDS. This shows that the lightweight classifier design, coupled with preprocessing and feature selection, significantly reduces the decision-making delay, enabling quicker threat mitigation at the edge and fog layers.

Energy Consumption

Energy efficiency is vital for battery-powered IoT devices. WiSIDS recorded 52% energy savings on NSL-KDD and 55% on Bot-IoT, in contrast to traditional IDS, which exhibited much higher resource consumption. These improvements validate the suitability of WiSIDS for deployment on constrained devices where energy optimization is a key requirement.

Overall Discussion

The integration of the Fog/Regional Layer also played a major role in improving system reliability by aggregating alerts across multiple gateways and applying ensemble models to reduce false positives. This contributed to a more scalable solution compared to single-point IDS implementations.

The experimental findings highlight that WiSIDS successfully balances high detection accuracy with low resource overhead, making it feasible for real-world wireless IoT environments. By combining optimized feature selection, lightweight classification, and hierarchical deployment across device, edge, fog, and cloud layers, WiSIDS addresses both the performance and practicality challenges of intrusion detection in IoT networks.

5. CONCLUSION

This paper introduced WiSIDS, a lightweight machine learning-based intrusion detection system designed to secure wireless IoT environments while addressing the unique limitations of

resource-constrained devices. Unlike traditional IDS solutions that demand high memory, processing power, and energy, WiSIDS combines feature selection with model optimization to deliver accurate detection without overwhelming system resources. The layered architecture—spanning IoT devices, edge gateways, fog nodes, and cloud management—ensures that intrusion detection is distributed intelligently, balancing real-time responsiveness with centralized learning and updates. Experimental results on NSL-KDD and Bot-IoT datasets demonstrated the effectiveness of WiSIDS, achieving detection accuracy above 95%, reducing latency by up to 60%, and lowering energy consumption by more than 50% compared to conventional IDS solutions. These outcomes highlight the system's practicality for real-world IoT deployments, where efficiency and security must coexist. Overall, WiSIDS proves that with the right balance of lightweight design and intelligent learning, it is possible to create scalable, resilient, and energy-efficient security solutions capable of safeguarding next-generation wireless IoT networks.

REFERENCES

[1] Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. *Sensors*, *23*(16), 7194.

[2] S.Gnanamurthy, & Santhosh Kumar Chenniappanadar. (2024). Enhancing Intrusion Detection using Deep Learning and An Improved Conditional Variational AutoEncoder (ICVAE). *IIRJET*, *8*(1). https://doi.org/10.32595/iirjet.org/v8i1.2022.162

[3] Chauhan, G. S., Jadon, R., & Awotunde, J. B. (2021). Smart IoT Analytics: Leveraging Device Management Platforms and Real-Time Data Integration with Self-Organizing Maps for Enhanced Decision-Making. *International Journal of Applied Science, Engineering, and Management*, *15*(2).

[4] Malik, S. (2024). Data-driven decision-making: leveraging the IoT for real-time sustainability in organizational behavior. *Sustainability*, *16*(15), 6302.

[5] Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. *IEEE access*, *8*, 23022-23040.

[6] Kizza, J. M. (2024). Internet of things (iot): growth, challenges, and security. In *Guide to computer network security* (pp. 557-573). Cham: Springer International Publishing.

[7] Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International journal of information security*, *22*(5), 1125-1162.

[8] Diana, L., Dini, P., & Paolini, D. (2025). Overview on Intrusion Detection Systems for Computers Networking Security. *Computers*, *14*(3), 87. https://doi.org/10.3390/computers14030087

[9] Slimani, C., Morge-Rollet, L., Lemarchand, L., Espes, D., Le Roy, F., & Boukhobza, J. (2025). A study on characterizing energy, latency and security for Intrusion Detection Systems on heterogeneous embedded platforms. *Future Generation Computer Systems*, *162*, 107473.

[10] Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. *Journal of Cloud Computing*, *13*(1), 123.

[11] Jouhari, M., & Guizani, M. (2024, May). Lightweight cnn-bilstm based intrusion detection systems for resource-constrained iot devices. In *2024 International Wireless Communications and Mobile Computing (IWCMC)* (pp. 1558-1563). IEEE.

[12] Wang, C., Xu, D., Li, Z., & Niyato, D. (2023). Effective intrusion detection in highly imbalanced IoT networks with lightweight S2CGAN-IDS. *IEEE Internet of Things Journal*, *11*(9), 15140-15151.

[13] Jouhari, M., Benaddi, H., & Ibrahimi, K. (2024, July). Efficient intrusion detection: Combining x 2 feature selection with CNN-BiLSTM on the UNSW-NB15 dataset. In *2024 11th International Conference on Wireless Networks and Mobile Communications (WINCOM)* (pp. 1-6). IEEE.

[14] Chu, H. C., & Lin, Y. J. (2023). Improving the IoT attack classification mechanism with data augmentation for generative adversarial networks. *Applied Sciences*, *13*(23), 12592.

[15] Qu, A., Shen, Q., & Ahmadi, G. (2024). Towards intrusion detection in fog environments using generative adversarial network and long short-term memory network. *Computers & Security*, *145*, 104004.