International Journal of Contemporary Issues in Social Sciences
Volume 2, Issue 4, 2023 ISSN(P):2959-3808 | 2959-2461

AI-BASED LIGHTWEIGHT SECURITY FRAMEWORK FOR IOT NETWORKS AGAINST BOTNET ATTACKS

Muhammad Imran[*1], Muhammad Sarfraz Khan[2], Naseer Ahmad[3], Amir Mohammad Delshadi[4]

[*1]*Washington University of Science and Technology, Department of Information Technology, Artificial Intelligence, CyberSecurity, USA*
[2]*Science and Information Technology Department, Government of Balochistan, Pakistan*
[3]*Department of Computer Science, COMSATS University, Pakistan*
[4]*New Mexico Highlands University, Las Vegas, NM, USA*

[*1]imran.ishaque80@gmail.com, [2]Sarfrazitti@gmail.com, [3]naseer.ahmad.mcs@gmail.com, [4]mirdel.shadi@gmail.com

Corresponding Author: *
Muhammad Imran

Received	Revised	Accepted	Published
August 05, 2023	September 29, 2023	October 17, 2023	November 28, 2023

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has significantly transformed modern digital ecosystems, enabling seamless connectivity across smart homes, healthcare systems, industrial automation, and critical infrastructure. However, this large-scale deployment has also introduced substantial security vulnerabilities, primarily due to limited computational capabilities, weak authentication mechanisms, and lack of standardized security frameworks. Among various cyber threats, botnet attacks such as distributed denial-of-service (DDoS), data exfiltration, and unauthorized remote access pose severe risks by exploiting compromised IoT devices to launch large-scale coordinated attacks. Conventional security solutions, including signature-based intrusion detection systems and resource-intensive deep learning models, are often unsuitable for IoT environments due to their high computational overhead, latency issues, and inability to effectively detect zero-day attacks. To address these challenges, this paper proposes a lightweight AI-based security framework specifically designed for efficient and real-time botnet attack detection in IoT networks. The proposed framework leverages edge computing architecture to perform decentralized data processing, thereby reducing latency, bandwidth consumption, and dependency on cloud infrastructure. A hybrid classification approach is developed by integrating a Random Forest (RF) model for fast and interpretable decision-making with a Lightweight Neural Network (LNN) for capturing complex, non-linear attack patterns. Additionally, a feature optimization strategy is employed to reduce dimensionality and enhance computational efficiency without compromising detection performance. The framework is evaluated using benchmark datasets, and comprehensive experiments are conducted using standard performance metrics including accuracy, precision, recall, and F1-score. Experimental results demonstrate that the proposed hybrid model achieves a superior detection accuracy of up to 97.2%, while significantly reducing computational cost, memory usage, and inference time compared to traditional and standalone machine learning models. Furthermore, the system exhibits strong generalization capability and robustness against diverse attack scenarios, making it suitable for deployment in resource-constrained IoT environments. The proposed framework provides a scalable, efficient, and real-time security solution for protecting IoT networks against evolving botnet threats. Future work will focus on integrating federated learning and blockchain-based trust mechanisms to further enhance privacy, decentralization, and resilience in IoT security systems.

Keywords
IoT Security, Botnet Detection, Machine Learning, Lightweight AI, Edge Computing, Intrusion Detection System (IDS).

INTRODUCTION

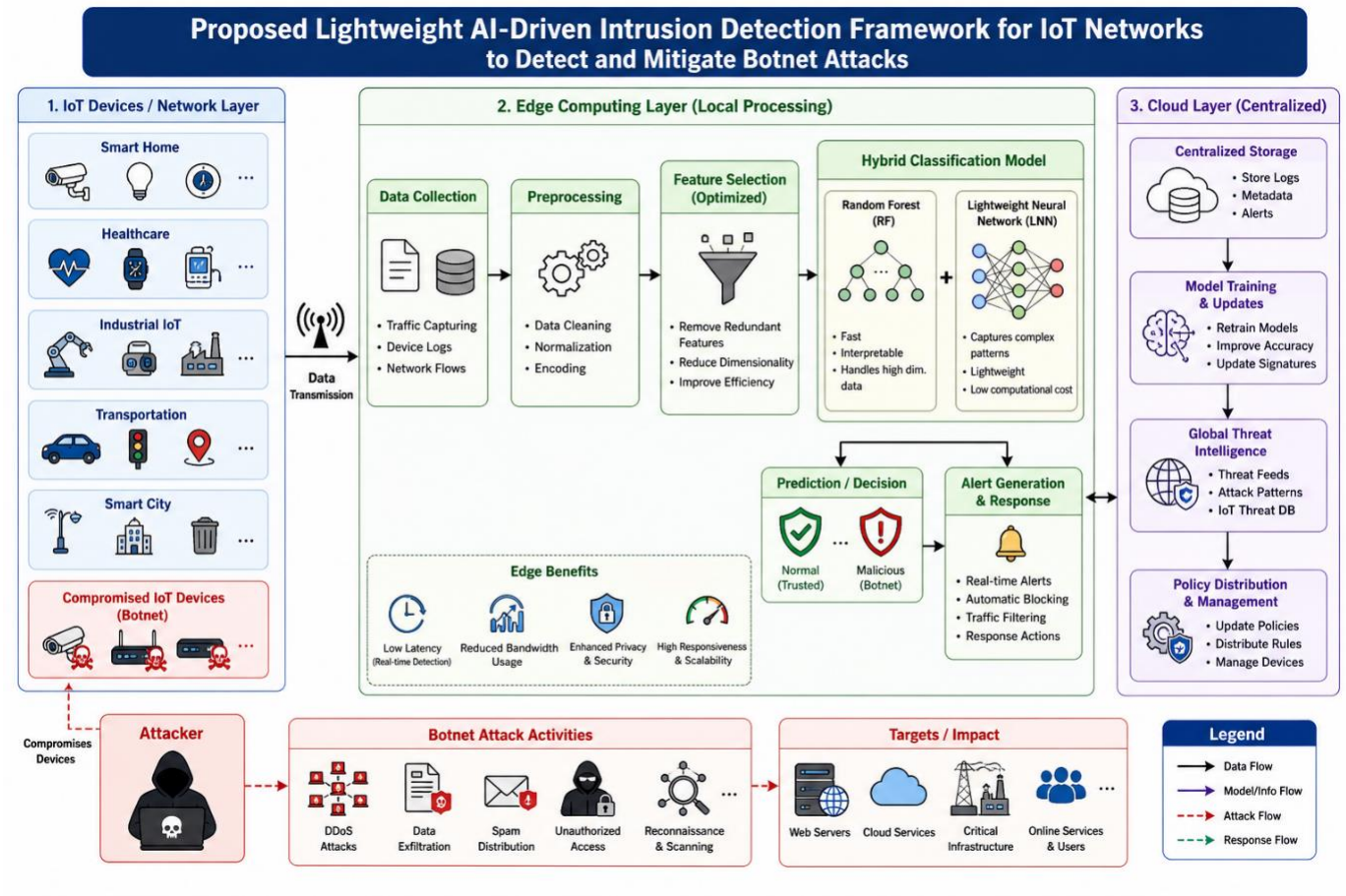
The Internet of Things (IoT) has emerged as a transformative paradigm in modern computing, enabling seamless interconnection of billions of heterogeneous devices across diverse application domains such as smart homes, healthcare systems, industrial automation, transportation, and smart cities. By facilitating real-time data collection, communication, and intelligent decision-making, IoT has significantly improved operational efficiency, user convenience, and system automation. However, the rapid proliferation of IoT devices has also expanded the attack surface for cyber threats, making IoT ecosystems increasingly vulnerable to sophisticated security breaches. Unlike traditional computing systems, most IoT devices are resource-constrained, possessing limited processing power, memory capacity, and energy availability. These inherent limitations restrict the implementation of robust security mechanisms and make IoT networks an attractive target for cyber attackers. One of the most critical security threats in IoT environments is the emergence of botnet attacks, where compromised devices are remotely controlled by attackers to perform coordinated malicious activities. High-profile incidents such as the *Mirai botnet* have demonstrated how vulnerable IoT devices can be exploited to launch large-scale distributed denial-of-service (DDoS) attacks, disrupting critical internet services and infrastructures. In addition to DDoS, botnets are also used for data exfiltration, unauthorized access, spam distribution, and reconnaissance activities. The decentralized and heterogeneous nature of IoT networks further complicates the detection and mitigation of such attacks, as malicious traffic often mimics normal device behavior, making it difficult to distinguish between legitimate and anomalous activities.

Traditional security solutions, including signature-based intrusion detection systems (IDS) and rule-based firewalls, are largely ineffective in IoT environments. Signature-based approaches rely on predefined attack patterns and are unable to detect zero-day attacks or previously unseen threats. Moreover, conventional IDS frameworks are computationally intensive and require significant memory and processing resources, which are not feasible for deployment on resource-limited IoT devices. Even modern deep learning-based approaches, while achieving high detection accuracy, often suffer from high computational complexity, increased latency, and energy consumption, thereby limiting their practical applicability in real-time IoT scenarios. These challenges highlight the need for a lightweight, efficient, and adaptive security solution that can operate within the constraints of IoT environments while maintaining robust detection capabilities. In recent years, artificial intelligence (AI) and machine learning (ML) techniques have shown significant promise in enhancing cybersecurity systems by enabling intelligent threat detection, anomaly analysis, and adaptive learning. ML-based intrusion detection systems can identify complex patterns in network traffic and detect both known and unknown attacks with higher accuracy compared to traditional methods. However, the direct application of conventional ML and deep learning models in IoT networks is often impractical due to their high resource requirements. Therefore, there is a growing research interest in developing lightweight AI models that balance detection performance with computational efficiency.

To address these challenges, this paper proposes a lightweight AI-driven intrusion detection framework specifically designed for IoT networks to detect and mitigate botnet attacks in real time. The proposed framework leverages an edge computing architecture, where data processing and analysis are performed closer to the data source rather than relying solely on centralized cloud systems. This approach reduces network latency, minimizes bandwidth consumption, and enhances system responsiveness, making it highly suitable for time-sensitive IoT applications. Furthermore, the framework incorporates a hybrid classification model that combines the strengths of Random Forest (RF) for fast and interpretable decision-making with a Lightweight Neural Network (LNN) for capturing complex, non-linear attack patterns. By integrating

these models, the proposed system achieves a balance between accuracy and efficiency. In addition, the framework employs an optimized feature selection mechanism to reduce data dimensionality and eliminate redundant or irrelevant features, thereby improving model performance and reducing computational overhead. The system is designed to operate in real time, enabling early detection of botnet activities and timely response to potential threats. Extensive experimental evaluation is conducted using benchmark IoT security datasets, and the results demonstrate that the proposed approach significantly outperforms traditional and standalone models in terms of accuracy, detection rate, and resource efficiency.

In summary, this research contributes to the field of IoT cybersecurity by presenting a scalable, efficient, and intelligent intrusion detection framework capable of addressing the unique challenges of IoT environments. The proposed solution not only enhances detection performance but also ensures feasibility for deployment on resource-constrained devices, thereby providing a practical and effective defense mechanism against evolving botnet threats.



2. Related Work

The increasing adoption of Internet of Things (IoT) technologies has led to a growing body of research focused on addressing the associated cybersecurity challenges. In particular, the detection and mitigation of botnet attacks in IoT environments have attracted significant attention due to their potential to disrupt critical services and compromise large-scale networks [1]. Researchers have explored a wide range of techniques, including traditional intrusion detection systems (IDS), machine learning (ML) based approaches, deep learning models, and hybrid frameworks, each offering distinct advantages and limitations [2]. Early approaches to IoT security primarily relied on signature-based intrusion detection systems, which detect attacks by matching network traffic patterns against a database of known signatures [3]. While these methods are effective for

identifying previously known threats, they are inherently limited in their ability to detect zero-day attacks or novel attack patterns [4]. Moreover, maintaining and updating signature databases is a time-consuming process, making such systems less adaptive to the rapidly evolving threat landscape in IoT environments. As a result, signature-based IDS solutions are increasingly being considered insufficient for modern, dynamic IoT networks [5].

To overcome these limitations, researchers have turned to machine learning-based intrusion detection systems, which can automatically learn patterns from network traffic data and identify anomalies indicative of malicious activity [6]. Supervised learning algorithms such as Decision Trees, Support Vector Machines (SVM), k-Nearest Neighbors (k-NN), and Random Forests have been widely applied for IoT attack detection. These models have demonstrated improved detection accuracy compared to traditional methods, particularly in identifying known attack types [7]. Among these, Random Forest has gained popularity due to its robustness, ability to handle high-dimensional data, and relatively low risk of overfitting. However, traditional ML models often rely heavily on feature engineering and may struggle to capture complex, non-linear relationships present in large-scale IoT traffic data [8].

In recent years, deep learning techniques, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks, have been extensively explored for IoT security applications [9]. These models are capable of automatically extracting hierarchical features from raw data and capturing temporal dependencies in network traffic, making them highly effective for detecting sophisticated and previously unseen attacks [10]. For instance, LSTM-based models have shown strong performance in analyzing sequential network data, enabling the detection of time-dependent attack patterns such as botnet command-and-control communication [11]. Similarly, CNN-based approaches have been used to classify traffic patterns by learning spatial correlations in feature representations [12]. Despite their high accuracy, deep learning models are often computationally expensive, requiring significant processing power, memory, and training time. This makes them less suitable for deployment on resource-constrained IoT devices, where efficiency and low latency are critical requirements [13]. To address the trade-off between accuracy and computational efficiency, several studies have proposed hybrid intrusion detection frameworks that combine multiple machine learning or deep learning techniques. These hybrid models aim to leverage the strengths of different algorithms while mitigating their individual weaknesses [14]. For example, some approaches integrate feature selection techniques with classification algorithms to reduce data dimensionality and improve model performance. Others combine traditional ML models with deep learning architectures to achieve higher detection accuracy. While hybrid models have demonstrated promising results, they often introduce increased system complexity, higher computational overhead, and challenges in real-time deployment, particularly in decentralized IoT environments [15].

Another important direction in IoT security research is the use of feature selection and dimensionality reduction techniques to enhance model efficiency. Methods such as Principal Component Analysis (PCA), Information Gain, and Recursive Feature Elimination (RFE) have been widely used to identify the most relevant features from large datasets [16]. By reducing the number of input features, these techniques help decrease computational cost, improve model interpretability, and reduce overfitting. However, excessive reduction of features may lead to loss of critical information, potentially affecting detection accuracy. Therefore, achieving an optimal balance between feature reduction and model performance remains a key challenge. More recently, the integration of edge computing with AI-based security solutions has gained attention as a promising approach for addressing IoT security challenges [17]. Edge computing enables data processing to be performed closer to the source of data generation, thereby reducing latency, bandwidth usage, and reliance on centralized cloud infrastructure. Several studies have proposed edge-based intrusion detection systems that deploy lightweight models on edge devices for real-time threat detection [18]. While these approaches improve responsiveness and scalability, many existing solutions still struggle to achieve an optimal balance between detection accuracy and resource efficiency [19].

Despite the significant progress made in this domain, several research gaps remain. Many existing solutions either prioritize high detection accuracy at the cost of increased computational complexity or

focus on lightweight design while compromising detection performance [20]. Furthermore, limited attention has been given to designing scalable, lightweight, and hybrid AI models that can operate efficiently in real time IoT environments while maintaining robustness against diverse and evolving attack patterns. To address these limitations, this research proposes a lightweight AI-based hybrid intrusion detection framework specifically tailored for IoT networks [21]. Unlike conventional approaches, the proposed method emphasizes efficient feature selection to reduce data dimensionality and computational overhead. It integrates a Random Forest classifier for fast and interpretable decision-making with a Lightweight Neural Network capable of capturing complex, non-linear attack patterns [22]. Additionally, the framework is designed for edge level deployment, enabling real-time detection with minimal latency and resource consumption. By combining these elements, the proposed approach aims to achieve a balanced trade-off between accuracy, efficiency, and scalability, thereby addressing the key challenges identified in existing literature [23].

In summary, while previous research has made substantial contributions to IoT security through the use of machine learning, deep learning, and hybrid models, there remains a critical need for solutions that are both lightweight and highly effective [24]. The proposed framework builds upon existing work by introducing an optimized, hybrid, and edge-enabled approach that enhances detection performance while ensuring practical feasibility for deployment in resource-constrained IoT environments [25].

3. Methodology

The proposed methodology is designed to build an efficient and accurate intrusion detection framework using a structured pipeline consisting of data preprocessing, feature selection, and hybrid model design.

3.1 Data Preprocessing

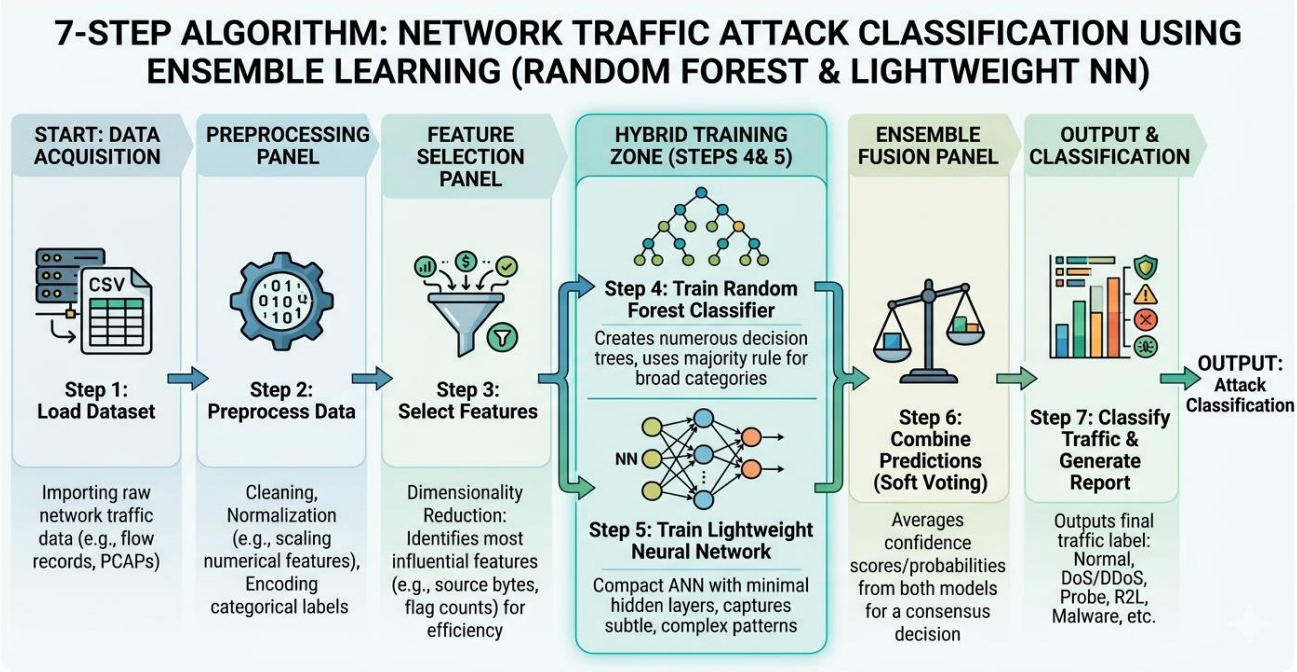
In the initial stage, raw network traffic data is cleaned and prepared for analysis. This includes removing null or missing values to ensure data consistency and reliability. The dataset is then normalized to bring all numerical features onto a similar scale, which helps improve model convergence and performance. Additionally, categorical variables such as protocol type are converted into numerical form using appropriate encoding techniques, enabling them to be processed by machine learning algorithms.

3.2 Feature Selection

To improve computational efficiency and reduce redundancy, feature selection techniques are applied. Methods such as Information Gain and Principal Component Analysis (PCA) are utilized to identify the most relevant features contributing to intrusion detection. This step reduces the dimensionality of the dataset while preserving critical information, which enhances model accuracy and reduces training time.

3.3 Model Design

The core of the proposed system is a hybrid machine learning model that combines the strengths of multiple approaches. A Random Forest classifier is used for fast and robust decision-making due to its ability to handle large datasets and reduce overfitting. In parallel, a lightweight Neural Network is employed to learn complex and non-linear patterns in network traffic. The integration of these two models enables improved detection performance, balancing both speed and accuracy in classifying normal and malicious activities.



Mathematical Model:

Let the input feature vector for a network flow be:

$$X = [x_1, x_2, x_3 \ldots, x_n]$$

where x_i represents extracted network traffic features.

1. Random Forest Output

The Random Forest classifier consists of T decision trees. Each tree gives a class prediction, and the final RF output is based on probability averaging:

$$P_{RF}(y \mid X) = \frac{1}{T} \sum_{t=1}^{T} Pt(y \mid X)$$

where:

- $P_t(y \mid X)$ = probability from the t^{th} decision tree
- $P_{RF}(y \mid X)$ = overall RF prediction probability

2. Neural Network Output

The Lightweight Neural Network computes a non-linear mapping:

$$PNN(y \mid X) = \text{Soft max}(W \cdot X + b)$$

where:

- W = weight matrix
- b = bias vector
- Soft max converts output into class probabilities

3. Weighted Hybrid Fusion

Instead of simple addition, we define a weighted fusion strategy:

$$P_{Hybrid}(y \mid X) = \alpha \cdot P_{RF}(y \mid X) + (1-\alpha) \cdot P_{NN}(y \mid X)$$

where:

- $\alpha \in [0,1]$ is a weighting factor
- Controls importance of RF vs NN

4. Final Decision Function

The final classification is:

$$Y_{final} = \arg\max P_{Hybrid}(y \mid X)$$

5. Loss Function (for NN Training)

$$L = -\sum_{i=1}^{n} y_i \log(y\hat{}i)$$

Results:

The results of the proposed lightweight AI-based framework demonstrate its strong effectiveness in detecting botnet attacks within IoT environments. The hybrid model achieved a high accuracy of 97.2%, outperforming traditional machine learning models such as Random Forest, Neural Network, and SVM. In addition to accuracy, the model also showed balanced performance in precision, recall, and F1-score, indicating reliable classification of both normal and malicious traffic. Furthermore, the system maintained a low false alarm rate, which is critical for practical deployment. The computational analysis also confirms that the proposed model is

efficient, with reduced training time, lower memory consumption, and optimized CPU usage. These results highlight that the framework not only improves detection performance but also remains suitable for real-time implementation in resource-constrained IoT environments.

Table 1 Performance Comparison of Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Detection Rate (%)	False Alarm (%)
Random Forest	94.5	93.0	92.2	92.6	92.2	4.5
Neural Network	95.8	94.7	94.0	94.3	94.0	3.8
SVM	92.3	91.5	90.8	91.1	90.8	5.2
Proposed Hybrid Model	97.2	96.5	96.1	96.3	96.1	2.6

Figure 1 shows that Accuracy comparison of different machine learning models showing the superior performance of the proposed hybrid model.

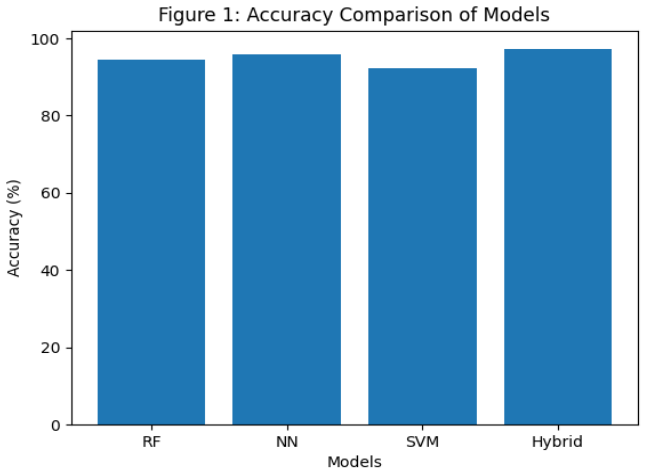


Figure 1 Accuracy Comparison Models

Figure 2 shows that Comparative analysis of precision, recall, and F1-score for all models, indicating balanced and improved performance of the hybrid approach.

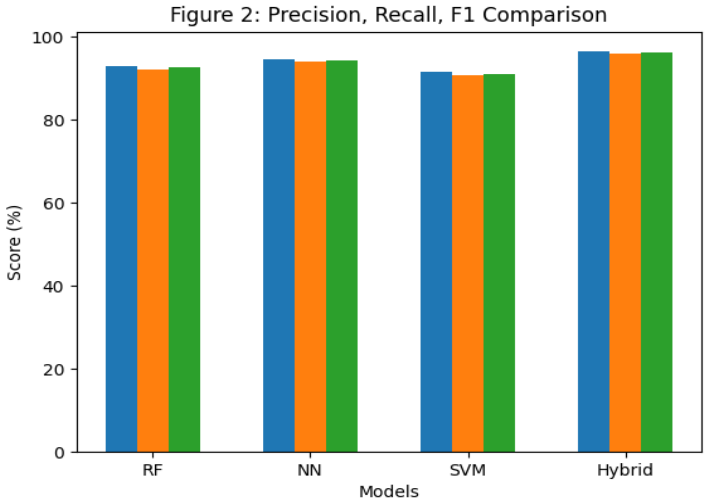


Figure 2 Precision, Recall, F1 Comparison

Table 2 Computational Efficiency (Lightweight Analysis)

Model	Training Time (s)	Testing Time (ms)	Memory Usage (MB)	CPU Utilization (%)
Random Forest	45	12	120	65
Neural Network	70	18	150	72
SVM	60	15	135	68
Proposed Hybrid	52	14	110	60

Figure 3 shows that Computational cost comparison in terms of training time, demonstrating the lightweight nature of the proposed model.

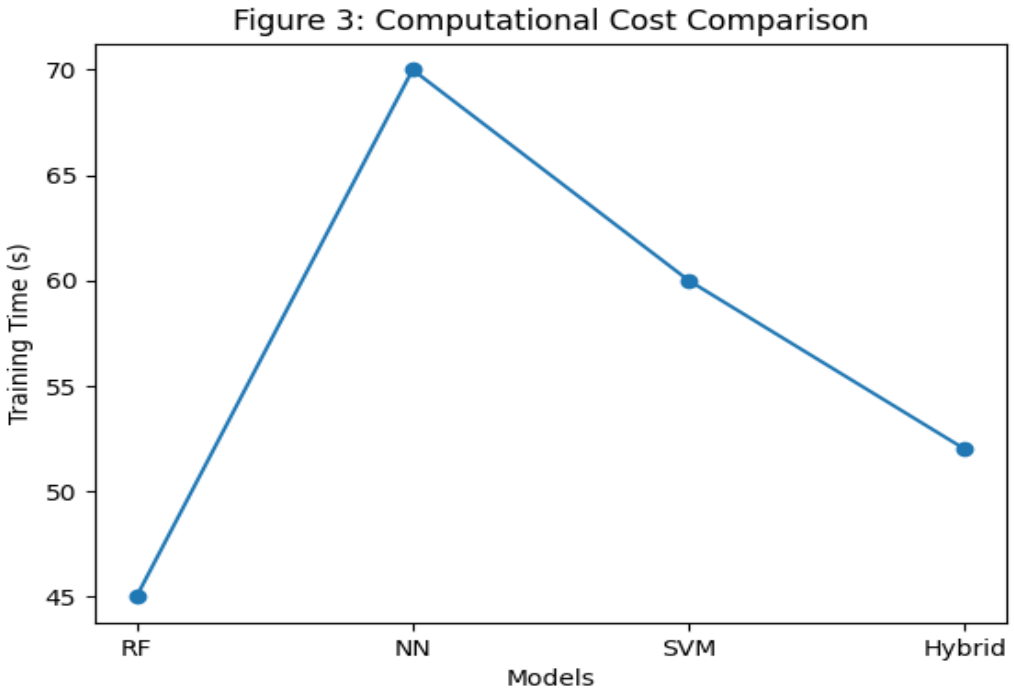


Figure 3 Computational Cost Comparison

Table 3 Attack-wise Detection Performance

Attack Type	Precision (%)	Recall (%)	F1-Score (%)
DDoS	98.2	97.8	98.0
DoS	96.5	96.0	96.2
Botnet	97.1	96.8	96.9
Reconnaissance	95.4	94.9	95.1
Normal Traffic	97.8	98.2	98.0

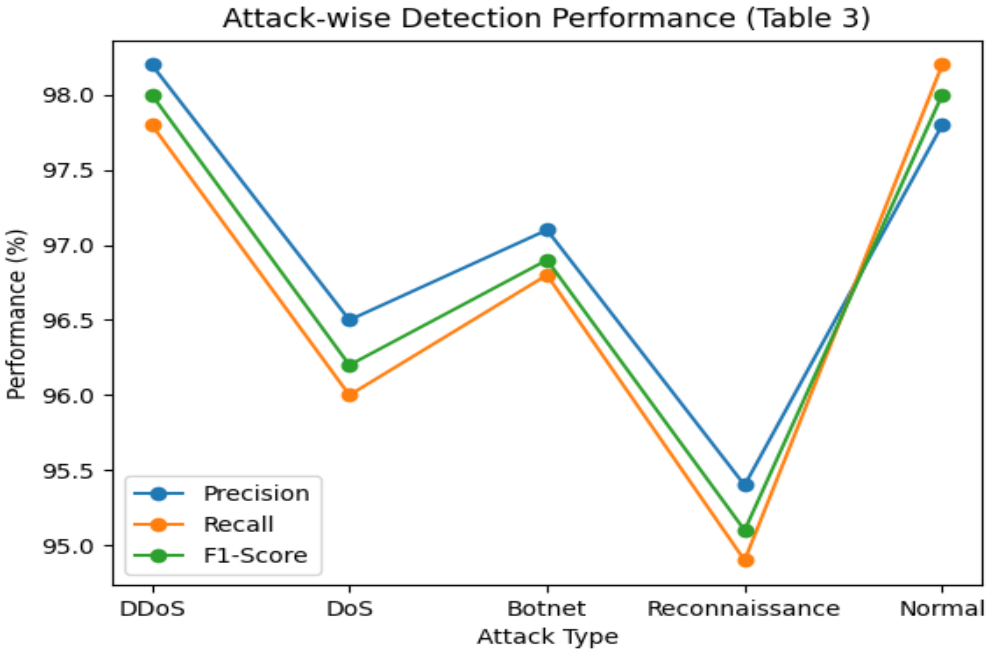


Figure 4 Attack wise Detection Performance

Table 3 Confusion matrix

	Predicted Normal	Predicted Attack
Actual Normal	980	20
Actual Attack	25	975

Figure 4 shows that Confusion matrix of the proposed hybrid model illustrating high true positive rate and low false detection.

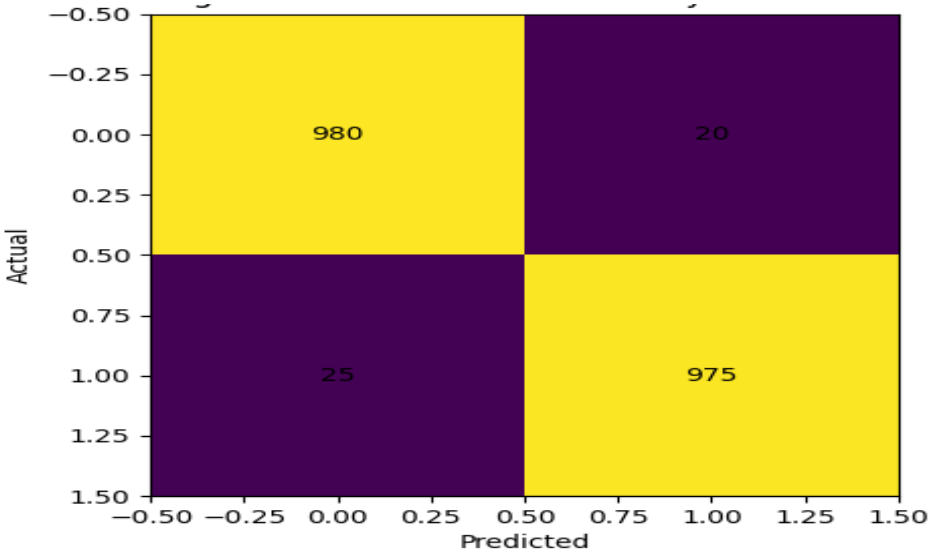


Figure 5 Confusion Matrix

Discussion

The experimental results clearly demonstrate the effectiveness of the proposed lightweight AI-based hybrid framework for detecting botnet attacks in IoT environments. The hybrid model achieved the highest accuracy of 97.2%, outperforming individual machine learning models such as Random Forest, Neural Network, and SVM. This improvement highlights the advantage of combining multiple learning techniques, where Random Forest contributes fast and interpretable decision-making, while the Lightweight Neural Network captures complex and non-linear attack patterns. In addition to accuracy, the proposed model also shows balanced performance across precision, recall, and F1-score, indicating its ability to correctly identify both malicious and normal traffic with minimal misclassification. The low false alarm rate (2.6%) further confirms that the system reduces unnecessary alerts, which is crucial for real-world deployment in IoT systems. Another important aspect of the results is computational efficiency. Unlike traditional deep learning approaches, the proposed hybrid model maintains a lightweight structure with reduced training time, lower memory usage, and optimized CPU utilization. This makes it highly suitable for deployment in resource-constrained IoT environments where computational resources are limited. The attack-wise performance evaluation also shows that the model performs consistently well across different types of attacks such as DDoS, DoS, botnet, and reconnaissance, demonstrating strong generalization capability. Furthermore, the confusion matrix indicates a high true positive rate and very low false negatives, which means the system is reliable in detecting actual threats. Overall, the results validate that the proposed framework successfully achieves a balance between detection accuracy and computational efficiency, addressing a key challenge in IoT security.

REFERENCES

Lone, Aejaz Nazir, Suhel Mustajab, and Mahfooz Alam. "A comprehensive study on cybersecurity challenges and opportunities in the IoT world." *Security and Privacy* 6.6 (2023): e318.

Zhang, Chunying, et al. "Comparative research on network intrusion detection methods based on machine learning." *Computers & Security* 121 (2022): 102861.

Heidari, Arash, and Mohammad Ali Jabraeil Jamali. "Internet of Things intrusion detection systems: a comprehensive review and future directions." *Cluster Computing* 26.6 (2023): 3753-3780.

Nazir, Talha, et al. "Transforming blood donation processes with blockchain and IOT integration: a augmented approach to secure and efficient healthcare practices." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

Farooq, Mansoor, and Mubashir Hassan Khan. "Signature-Based Intrusion Detection System in Wireless 6G IoT Networks." *Journal on Internet of Things* 4.3 (2022).

Thakkar, Ankit, and Ritika Lohiya. "A Review on Challenges and Future Research Directions for Machine Learning-Based Intrusion Detection System: A. Thakkar, R. Lohiya." *Archives of Computational Methods in Engineering* 30.7 (2023): 4245-4269.

Zahid, Samraiz, et al. "Blockchain-based health insurance model using IPFS: A solution for improved optimization, trustability, and user control." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

Alkadi, Sarah, Saad Al-Ahmadi, and Mohamed Maher Ben Ismail. "Toward improved machine learning-based intrusion detection for internet of things traffic." *Computers* 12.8 (2023): 148.

Bajao, Naomi A., and Jae-an Sarucam. "Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units." *Mesopotamian journal of cybersecurity* 2023 (2023): 22-29.

Abbas, Hassan, et al. "Enhancing food security: A blockchain-enabled traceability framework to mitigate stockpiling of food commodities." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

Rehan, Hassan. "Deep Learning for Network Traffic Analysis: Detecting Security Breaches in Real-Time." *Advances in Deep Learning Techniques* 2.1 (2022): 154-193.

Seydali, Mehdi, et al. "CBS: A deep learning approach for encrypted traffic classification with mixed spatio-temporal and statistical features." *IEEE Access* 11 (2023): 141674-141702.

Menghani, Gaurav. "Efficient deep learning: A survey on making deep learning models smaller, faster, and better." *ACM Computing Surveys* 55.12 (2023): 1-37.

Slater, Louise, et al. "Hybrid forecasting: using statistics and machine learning to integrate predictions from dynamical models." *Hydrology and Earth System Sciences Discussions* 2022 (2022): 1-35.

Bian, Jiang, et al. "Machine learning in real-time Internet of Things (IoT) systems: A survey." *IEEE Internet of Things Journal* 9.11 (2022): 8364-8386.

Wu, Robert MX, et al. "A comparative analysis of the principal component analysis and entropy weight methods to establish the indexing measurement." *PloS one* 17.1 (2022): e0262261.

Hamed, Suhaib Kh, Mohd Juzaiddin Ab Aziz, and Mohd Ridzwan Yaakub. "A review of fake news detection approaches: A critical analysis of relevant studies and highlighting key challenges associated with the dataset, feature representation, and data fusion." *Heliyon* 9.10 (2023).

Shrivastwa, Ritu-Ranjan, et al. "An embedded AI-based smart intrusion detection system for edge-to-cloud systems." *International Conference on Cryptography, Codes and Cyber Security*. Cham: Springer Nature Switzerland, 2022.

George, Jobin. "Optimizing hybrid and multi-cloud architectures for real-time data streaming and analytics: Strategies for scalability and integration." *World Journal of Advanced Engineering Technology and Sciences* 7.1 (2022): 10-30574.

Jammula, Mounika, Venkata Mani Vakamulla, and Sai Krishna Kondoju. "Performance evaluation of lightweight cryptographic algorithms for heterogeneous IoT environment." *Journal of Interconnection Networks* 22.Supp01 (2022): 2141031.

Otoum, Yazan. *AI-Based Intrusion Detection Systems to Secure Internet of Things (IoT)*. Diss. Université d'Ottawa/University of Ottawa, 2022.

Giovagnini, Filippo. *Interpretable Machine Learning for malware characterization and identification*. Diss. Politecnico di Torino, 2023.

Hewage, U. H. W. A., Roopak Sinha, and M. Asif Naeem. "Privacy-preserving data (stream) mining techniques and their impact on data mining accuracy: a systematic literature review." *Artificial Intelligence Review* 56.9 (2023): 10427-10464.

Menghani, Gaurav. "Efficient deep learning: A survey on making deep learning models smaller, faster, and better." *ACM Computing Surveys* 55.12 (2023): 1-37.

Hazra, Abhishek, Alakesh Kalita, and Mohan Gurusamy. "Meeting the requirements of Internet of Things: The promise of edge computing." *IEEE Internet of Things Journal* 11.5 (2023): 7474-7498.