



An Explainable Two-Stage Lightweight Deep Learning Framework for IoT Botnet Attack Detection Using BorutaSHAP

¹Neelendra Shekhar Gupta, ²Satendra Kumar Jain

¹MTech Scholar, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal

²Assistant professor, Department of Computer Science and Engineering, Lakshmi Narain College of Technology, Bhopal

¹neelendrashekhar@gmail.com, ²satendrakj@lnct.ac.in

Abstract: - IoT networks are increasingly exposed to sophisticated botnet attacks that typically evolve through multiple stages, beginning with reconnaissance (scan) activities and progressing toward large-scale Distributed Denial of Service (DDoS) attacks. To address these challenges, this study proposes a two-fold intelligent detection framework for early identification and mitigation of IoT botnet attacks in heterogeneous network environments. The existing approaches are limited in their ability to handle multi-stage attack progression and often rely on heavy deep learning architectures, leading to higher computational complexity and reduced adaptability across diverse datasets. The proposed methodology introduces a sequential detection strategy comprising two stages: scan detection and DDoS detection. In the first stage, a lightweight MobileNetV3-Small model is utilized to identify scanning activities during the reconnaissance phase, while in the second stage, an EfficientNetV2-B0 model is employed for detecting DDoS attacks in compromised IoT environments. To enhance feature relevance and eliminate redundancy, BorutaSHAP-based feature selection is applied, which integrates Boruta and SHAP importance measures to identify the most significant network flow features. The framework further incorporates SHAP-based explainability to improve model interpretability by quantifying feature contributions to classification decisions. The system is evaluated using three benchmark datasets CICIDS2017, CICIDS2019, and Bot-IoT along with two self-generated datasets, ScanLab and DDoSLab. Network traffic is processed using CICFlowMeter and transformed into structured flow-based representations. Experimental results demonstrate strong performance, with BorutaSHAP-based surrogate models achieving accuracy above 99%, while the lightweight CNN models maintain stable performance around 92% accuracy for both scan and DDoS detection tasks. Overall, the proposed framework achieves a balance between detection accuracy, computational efficiency, and interpretability, making it effective for multi-stage IoT botnet attack detection scenarios.

Keywords: IoT Botnet Detection, BorutaSHAP Feature Selection, MobileNetV3-Small, EfficientNetV2-B0, Explainable Artificial Intelligence (SHAP).

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices across smart homes, healthcare systems, industrial automation, transportation, and critical infrastructure has significantly transformed modern digital ecosystems by enabling seamless connectivity and intelligent



decision-making. However, the increasing deployment of interconnected IoT devices has simultaneously expanded the cyberattack surface, making IoT environments highly vulnerable to sophisticated security threats, particularly botnet attacks [1]. IoT botnets exploit weak authentication mechanisms, outdated firmware, and inadequate security configurations to compromise devices and coordinate malicious activities on a large scale. These attacks generally follow a multi-stage lifecycle, beginning with reconnaissance or scanning activities to identify vulnerable devices, followed by malware propagation and culminating in large-scale Distributed Denial of Service (DDoS) attacks that can disrupt services, degrade network performance, and cause substantial economic losses. Existing intrusion detection approaches primarily focus on identifying attacks during the final stages of execution and often rely on computationally intensive models that are unsuitable for resource-constrained IoT environments [2]. Furthermore, many existing methods adopt a single-stage detection strategy and exhibit limited adaptability across heterogeneous datasets, thereby reducing their effectiveness in real-world deployments. Detecting multi-stage IoT botnet attacks remains challenging due to the dynamic nature of network traffic, high variability in attack patterns, class imbalance issues, feature redundancy, and the need to achieve a balance between detection accuracy and computational efficiency. In particular, scanning activities exhibit subtle behavioral characteristics that are difficult to distinguish from legitimate traffic, making early-stage attack detection a complex task [3]. Similarly, DDoS attacks generate highly diverse traffic patterns that require robust and generalized detection mechanisms. Another major limitation of contemporary deep learning-based intrusion detection systems is the lack of interpretability, which restricts their adoption in security-critical applications where transparent decision-making is essential. Consequently, there is an increasing demand for intelligent, lightweight, and explainable frameworks capable of identifying attacks at multiple stages while maintaining high performance across diverse environments. Motivated by these challenges, the present study proposes an explainable two-stage lightweight deep learning framework for IoT botnet attack detection using BorutaSHAP-based feature selection [4]. The proposed framework introduces a sequential detection strategy in which MobileNetV3-Small is employed to identify malicious scanning activities during the reconnaissance phase, while EfficientNetV2-B0 is utilized to detect DDoS attacks generated by compromised IoT devices. To enhance feature relevance and eliminate redundant information, the BorutaSHAP algorithm is integrated to select statistically significant network flow features, thereby improving model efficiency and interpretability. Additionally, SHAP-based explainable artificial intelligence techniques are incorporated to provide both local and global explanations of classification decisions, enhancing transparency and trustworthiness. The framework is evaluated using multiple benchmark datasets, including CICIDS2017, CICIDS2019, and Bot-IoT, together with self-generated ScanLab and DDoSLab datasets to ensure cross-dataset validation and robust generalization [5]. The primary objectives of this research are to facilitate early detection of scan and DDoS attacks, develop computationally efficient lightweight convolutional neural network models, improve feature selection through BorutaSHAP, enhance model

interpretability using SHAP, and validate the proposed methodology across heterogeneous datasets. Overall, the proposed framework contributes toward the development of efficient, scalable, and explainable IoT security solutions capable of addressing the evolving challenges of multi-stage botnet attack detection in modern interconnected environments.

II. LITERATURE REVIEW

Recent advances in IoT botnet detection have increasingly focused on developing scalable, interpretable, and computationally efficient intrusion detection frameworks. Sagu et al. [1] proposed a scalable and interpretable deep learning-based intrusion detection framework for secure IoT networks, emphasizing explainability and robust performance across heterogeneous environments. Similarly, Vishnu and Singh [2] introduced a hybrid multi-model ensemble framework that demonstrated improved threat detection capabilities against diverse network intrusion attacks through ensemble learning strategies. Saied and Guirguis [3] highlighted the importance of Explainable Artificial Intelligence (XAI) in IoT botnet detection by integrating SHAP-based explanations to enhance transparency and trust in security decisions. Bobade et al. [4] developed a DBN-RNN-based intelligent detection framework with an improved feature set, achieving high detection performance while addressing feature redundancy challenges. Likewise, Ashok Kumar and Kanagachidambaresan [5] proposed a combined deep learning framework using selective feature extraction techniques to improve botnet attack detection in IoT environments.

Recent studies have also explored lightweight architectures and advanced feature selection methods. Badr et al. [7] optimized FastViT using Boruta-SHAP and class balancing techniques for lightweight cloud-based multiclass intrusion detection, demonstrating the effectiveness of explainable feature selection approaches. EL ASRY [9] investigated advanced intrusion detection by integrating sequential learning, semantic analysis, and graph-based representations, highlighting the benefits of combining multiple learning paradigms. Kalidindi and Arrama [10] introduced a hybrid CNNF deep stacked autoencoder with feature selection for IoT botnet detection, while Hossain and Islam [11] proposed a privacy-preserving federated learning framework to support decentralized botnet detection. Rupanetti and Kaabouch [12] further explored machine learning techniques for edge-computing-assisted IoT networks, emphasizing the need for lightweight and deployable security models. Wasswa et al. [13] presented a latent space alignment approach to improve robustness in non-stationary environments, whereas Polam et al. [14] demonstrated the effectiveness of advanced machine learning techniques in addressing evolving cyber threats.

Feature engineering and optimization techniques have also attracted significant attention. Sheheryar and Sharma [15] employed ensemble feature engineering with deep learning for improved botnet detection performance, while Bindu et al. [16] utilized the American Zebra Optimization Algorithm with SSRNN-ELM for software-defined IoT networks. Gelgi et al. [17] conducted a systematic review of IoT botnet DDoS attacks and concluded that lightweight and explainable approaches remain underexplored. Alshaeaa and Ghadhban [18,20] proposed a hybrid feature selection method to improve attack detection accuracy. Earlier studies by



Habibi et al. [21,22], Saif et al. [23], Muñoz and Valiente [24], and Jakkani et al. [25] demonstrated the effectiveness of machine learning, communication graph analysis, and deep learning methodologies for IoT botnet detection. Despite these advancements, existing approaches are often limited by high computational complexity, insufficient explainability, and inadequate validation across multiple datasets. Therefore, there remains a need for a lightweight, interpretable, and cross-dataset validated framework capable of detecting multiple stages of IoT botnet attacks, which serves as the primary motivation for the proposed research.

III. RESEARCH METHODOLOGY

This section presents the datasets, preprocessing steps, feature selection, lightweight deep learning models, and explainability techniques used for IoT botnet detection.

A. Dataset Description

The proposed study utilizes three publicly available benchmark datasets, namely CICIDS2017, CICIDS2019, and Bot-IoT, together with two self-generated datasets, ScanLab and DDoSLab, to ensure attack diversity and robust model evaluation. The benchmark datasets provide normal, scanning, and DDoS traffic collected from realistic network environments, while ScanLab contains 33 scanning attack types and DDoSLab consists of 60 DDoS attack variations. Network traffic is captured in PCAP format and transformed into flow-level records using CICFlowMeter, which extracts more than 60 statistical network flow features. These datasets collectively support comprehensive training, testing, and cross-dataset validation of the proposed framework.

B. Data Preprocessing

Data preprocessing is performed to improve data quality and ensure consistency among heterogeneous datasets. Initially, the required traffic records are extracted and divided into two subsets: Scan Detection Dataset containing benign and scanning traffic, and DDoS Detection Dataset comprising benign and DDoS traffic. Feature harmonization is subsequently conducted to standardize feature names and ordering across all datasets. Non-informative attributes such as flow identifiers, timestamps, IP addresses, and port numbers are removed to prevent model bias. Missing and infinite values are identified and replaced using median-based imputation to maintain numerical stability. Legitimate traffic outliers are retained as they represent significant attack signatures. Following data cleaning, the selected features are normalized using Min-Max scaling to maintain uniform value ranges. Finally, the processed datasets are transformed into $32 \times 32 \times 3$ RGB image representations and partitioned into training (60%), validation (20%), and testing (20%) subsets.

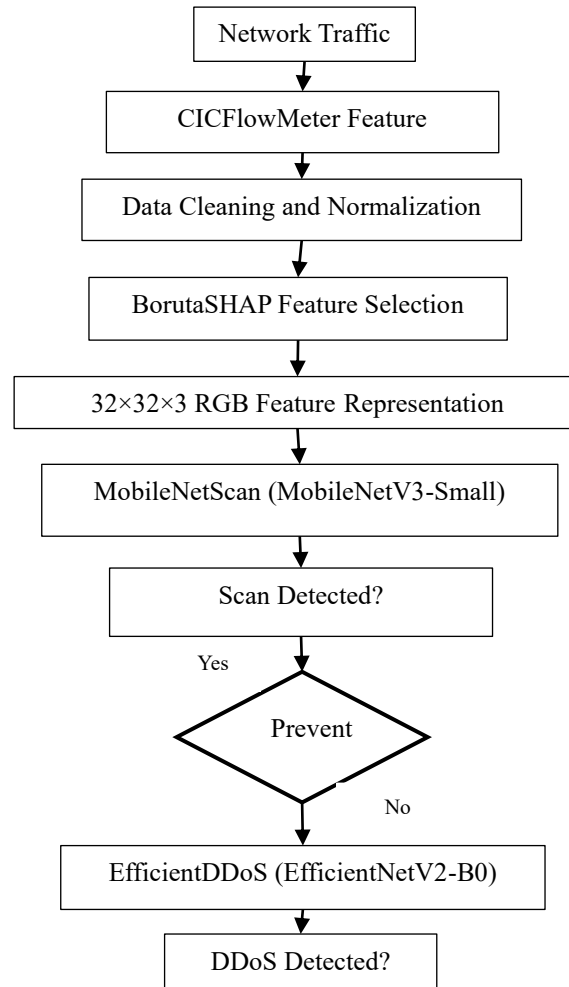


Figure 1. Proposed enhanced two-fold architecture based on BorutaSHAP, MobileNetV3-Small, EfficientNetV2-B0, and SHAP for early prevention and detection of IoT botnet attacks.

Figure 1 illustrates the proposed enhanced two-fold IoT botnet detection architecture designed for the early prevention and detection of multi-stage attacks. The framework begins with network traffic collection, where raw packets are processed using CICFlowMeter to extract flow-based features. These features undergo data cleaning, normalization, and BorutaSHAP-based feature selection to retain only the most significant attributes. The selected features are transformed into $32 \times 32 \times 3$ RGB image representations and forwarded to the first detection stage, MobileNetV3-Small (MobileNetScan), which identifies malicious scanning activities during the reconnaissance phase. If a scanning attack is detected, preventive actions are initiated immediately; otherwise, the traffic is passed to the second stage, EfficientNetV2-B0 (EfficientDDoS), for DDoS attack detection. Finally, SHAP-based explainability is employed to provide interpretable insights into the classification decisions made by both models. Overall, the architecture provides a lightweight, explainable, and computationally efficient solution for detecting IoT botnet attacks across multiple stages of the attack lifecycle.

C. BorutaSHAP Feature Selection

To improve feature relevance and reduce computational complexity, the proposed framework employs BorutaSHAP-based feature selection. BorutaSHAP combines the Boruta wrapper algorithm with SHAP importance estimation to identify statistically significant and attack-relevant network flow features. Unlike conventional feature selection methods, BorutaSHAP evaluates feature importance by comparing original attributes against randomly generated shadow features. The feature selection process begins by creating shadow copies through random permutation of existing features. An ensemble learning model is then trained using both original and shadow features, after which SHAP values are computed to quantify the contribution of each feature toward classification decisions. Features consistently outperforming their shadow counterparts are retained, while redundant and non-informative attributes are discarded. This process enhances model interpretability by selecting features that contribute significantly to attack discrimination. Furthermore, BorutaSHAP reduces dimensionality, minimizes overfitting, and improves computational efficiency by eliminating unnecessary information. The selected features are subsequently utilized by both the scan detection and DDoS detection modules, ensuring a unified and optimized feature space. Overall, BorutaSHAP plays a critical role in improving classification performance while maintaining transparency and robustness within the proposed IoT botnet detection framework.

D. MobileNetV3-Small

The first stage of the proposed framework utilizes MobileNetV3-Small to detect malicious scanning activities during the reconnaissance phase of IoT botnet attacks. MobileNetV3-Small is selected due to its lightweight architecture, reduced parameter count, and efficient feature extraction capabilities, making it highly suitable for resource-constrained IoT environments. The model receives BorutaSHAP-selected network flow features transformed into $32 \times 32 \times 3$ RGB image representations. MobileNetV3-Small incorporates depthwise separable convolutions, squeeze-and-excitation attention mechanisms, and hard-swish activation functions to achieve an optimal balance between accuracy and computational efficiency. The output layer performs binary classification by categorizing incoming traffic as either Normal or Scanning traffic. By identifying reconnaissance activities at an early stage, the model enables proactive mitigation of IoT botnet attacks before they progress to subsequent attack phases. The scan detection module is referred to as MobileNetScan within the proposed framework.

E. EfficientNetV2-B0

The second stage of the proposed framework employs EfficientNetV2-B0 for DDoS attack detection. This model is activated when scanning activities evade the first-stage detection mechanism and compromised IoT devices begin generating malicious traffic. EfficientNetV2-B0 is selected due to its efficient compound scaling strategy and fused MBConv blocks, which provide an improved trade-off between model complexity and classification performance. Similar to the scan detection model, EfficientNetV2-B0 receives BorutaSHAP-selected features represented as $32 \times 32 \times 3$ RGB images. The model performs binary classification by distinguishing between Normal and DDoS traffic. Its lightweight design ensures reduced

computational overhead while maintaining robust detection capabilities across diverse attack patterns. By accurately identifying malicious traffic generated by compromised devices, EfficientNetV2-B0 strengthens the overall two-stage detection strategy and enhances the resilience of the proposed IoT botnet detection framework in heterogeneous network environments.

F. SHAP Explainability Framework

To improve transparency and interpretability, the proposed framework integrates SHAP (SHapley Additive exPlanations) as an explainable artificial intelligence component. SHAP quantifies the contribution of each selected feature toward individual classification decisions generated by MobileNetV3-Small and EfficientNetV2-B0. The framework provides both local explanations for individual predictions and global explanations that summarize feature importance across the entire dataset. For scan detection, SHAP identifies features such as Initial Forward/Backward Window Bytes, Flow IAT Minimum, and Packet Length statistics as significant contributors to attack classification. Similarly, for DDoS detection, Average Packet Size, Packet Length Mean, and Backward Packets per Second are identified as influential features. By providing clear insights into model behavior, SHAP enhances trustworthiness and facilitates the interpretation of complex deep learning decisions. Consequently, the integration of SHAP enables the proposed framework to achieve improved explainability while maintaining strong detection performance across multiple IoT botnet attack scenarios.

G. Performance Metrics

1. Accuracy

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

2. Precision

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

3. Recall (Detection Rate)

$$\text{Recall} = \frac{TP}{TP+FN} \quad (3)$$

4. F1-Score

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (4)$$

5. Area Under the ROC Curve (AUC-ROC)

$$\text{AUC} \in [0,1] \quad (5)$$

Where: AUC = 1.0 indicates perfect classification, AUC = 0.5 indicates random guessing.

H. Parameter Count

Parameter count measures the total number of trainable parameters present within a deep learning model and serves as an indicator of model complexity.

Table 1. Comparison of Trainable Parameters for Different Deep Learning Models

Model	Trainable Parameters
ResNet-18	11.18 Million
MobileNetV3-Small	2.54 Million
EfficientNetV2-B0	7.10 Million

I. Inference Time

$$\text{Inference Time} = \frac{\text{Total Prediction Time}}{\text{Number of Test Samples}} \quad (6)$$

IV. RESULTS AND DISCUSSION

The performance of the proposed BorutaSHAP + MobileNetV3-Small + EfficientNetV2-B0 framework is evaluated using both surrogate machine learning models and deep learning models. The results demonstrate the effectiveness of the proposed feature selection strategy and lightweight CNN architectures for IoT botnet attack detection. The BorutaSHAP-based surrogate models (Random Forest) achieve very high performance, with 99.43% accuracy for scan detection and 99.61% accuracy for DDoS detection, indicating that the selected features are highly discriminative. For deep learning models, the MobileNetV3-Small scan detection model achieves an accuracy of 92.61%, while the EfficientNetV2-B0 DDoS detection model achieves an accuracy of 92.20%. These results confirm that even with lightweight architectures, the proposed framework maintains strong classification capability while significantly reducing computational complexity. Table 1 compares the performance of the proposed two-fold framework, demonstrating that BorutaSHAP-based models achieve over 99% accuracy, while lightweight CNN models provide efficient and reliable IoT botnet detection.

Table 2 Performance Comparison of Proposed Two-Fold Framework

Component	Accuracy	F1-Score
BorutaSHAP → RF Surrogate (Scan)	99.43%	99.43%
BorutaSHAP → RF Surrogate (DDoS)	99.61%	99.61%
MobileNetV3-Small CNN (Scan Fold)	92.61%	92.62%
EfficientNetV2-B0 CNN (DDoS Fold)	92.20%	92.47%

A. Confusion Matrix of Proposed Lightweight IoT Botnet Detection Framework

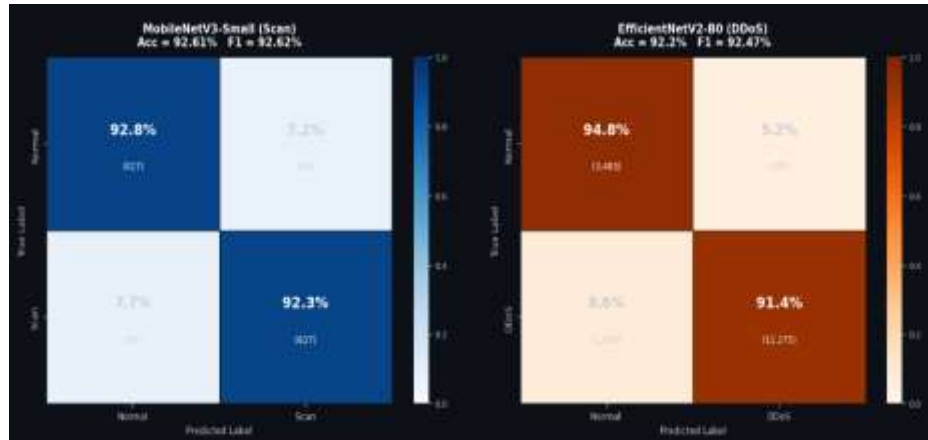


Figure 2 Confusion Matrix of Proposed Lightweight IoT Botnet Detection Framework

The above figure 2 represents the normalized confusion matrices of the proposed lightweight IoT botnet detection framework, which includes MobileNetV3-Small for scan detection and EfficientNetV2-B0 for DDoS detection. The confusion matrices provide a detailed visualization of classification performance by showing correct and incorrect predictions for each class. For the MobileNetV3-Small scan detection model, the results show that 92.8% of normal traffic is correctly classified, while 92.3% of scan traffic is correctly identified. A small percentage of misclassifications is observed, where 7.2% of normal traffic is incorrectly classified as scan traffic and 7.7% of scan traffic is misclassified as normal. This indicates that the model achieves balanced performance in detecting reconnaissance activities while maintaining stability across both classes. For the EfficientNetV2-B0 DDoS detection model, 94.8% of normal traffic is correctly classified and 91.4% of DDoS traffic is correctly identified. The misclassification rates remain relatively low, with 5.2% of normal traffic classified as DDoS and 8.6% of DDoS traffic classified as normal. This demonstrates that the model is effective in distinguishing between benign and malicious DDoS traffic, although DDoS classification shows slightly higher complexity compared to scan detection. Overall, both models exhibit strong diagonal dominance in the confusion matrices, confirming that the proposed framework achieves reliable classification performance. The results validate the effectiveness of using lightweight architectures such as MobileNetV3-Small and EfficientNetV2-B0 for efficient IoT botnet attack detection while maintaining competitive accuracy.

B. Performance Analysis of Proposed Framework

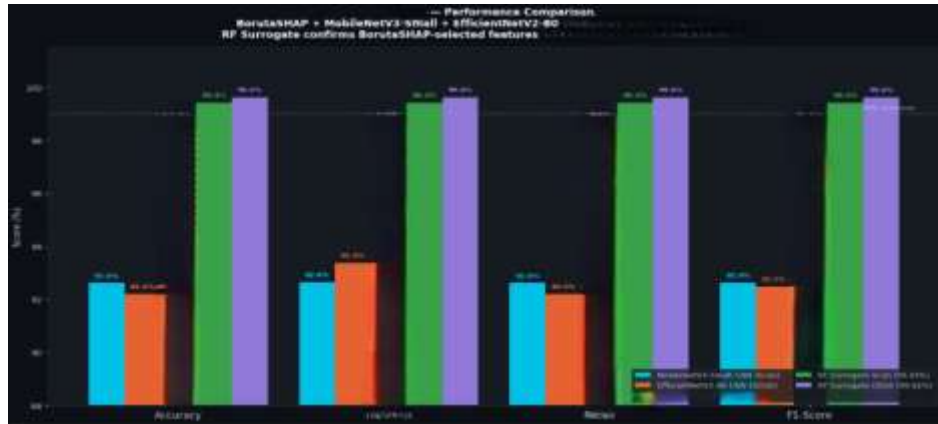


Figure 3 Performance Analysis of Proposed Framework

The above figure 3 illustrates the performance evaluation of the proposed BorutaSHAP + MobileNetV3-Small + EfficientNetV2-B0 framework across four key classification metrics: Accuracy, Precision, Recall, and F1-score for both scan detection and DDoS detection tasks. The results show that the MobileNetV3-Small scan detection model achieves a consistent performance of approximately 92.6% accuracy, with closely matched precision, recall, and F1-score values. This indicates that the model maintains a balanced ability to correctly identify both normal and scanning traffic without significant bias toward any single class. Similarly, the EfficientNetV2-B0 DDoS detection model demonstrates slightly lower but stable performance, with an accuracy of around 92.2% to 93.4% across metrics. The close alignment between precision, recall, and F1-score indicates that the model is consistently performing well in detecting DDoS attack patterns while maintaining low misclassification rates. Overall, the figure highlights that both models in the proposed framework maintain balanced and stable classification performance across all evaluation metrics, demonstrating the effectiveness of the lightweight architecture and BorutaSHAP-based feature selection in enhancing IoT botnet attack detection.

C. SHAP-Based Feature Importance Analysis for Scan and DDoS Detection

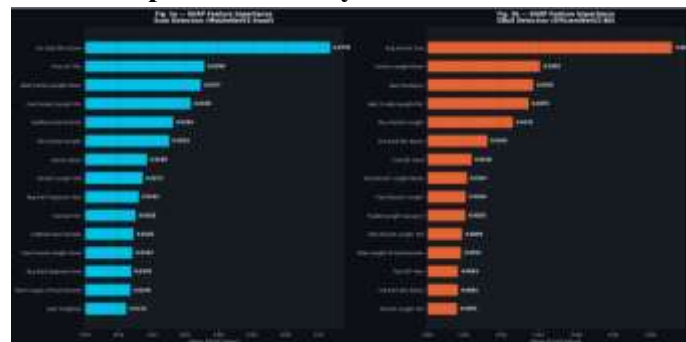


Figure 4 SHAP-Based Feature Importance Analysis for Scan and DDoS Detection

The above figure 4 presents the SHAP-based feature importance analysis for both scan detection and DDoS detection tasks in the proposed framework. SHAP (SHapley Additive

explanations) is used to quantify the contribution of each network flow feature toward the final prediction of the model.

D. Comparative Performance Analysis of Existing and Proposed IoT Botnet Detection Frameworks

Table 3 Comparative Performance Analysis of Existing and Proposed IoT Botnet Detection Frameworks

Model / System	Accuracy	Precision	Recall	F1-Score
ResNetScan-1	95.10%	95.48%	95.10%	95.12%
ResNetDDoS-1	97.93%	97.97%	97.93%	97.94%
Overall (Existing Combined)	96.52%	96.72%	96.52%	96.53%
BorutaSHAP → RF (Scan)	99.43%	—	—	99.43%
BorutaSHAP → RF (DDoS)	99.61%	—	—	99.61%
MobileNetV3-Small (Scan Fold)	92.61%	—	—	92.62%
EfficientNetV2-B0 (DDoS Fold)	92.20%	—	—	92.47%

The above table 2 presents a comprehensive comparison between the existing ResNet-18 based two-fold IoT botnet detection framework and the proposed lightweight framework utilizing BorutaSHAP feature selection along with MobileNetV3-Small and EfficientNetV2-B0 models.

E. Comparative Performance Analysis of Existing and Proposed IoT Botnet Detection Frameworks

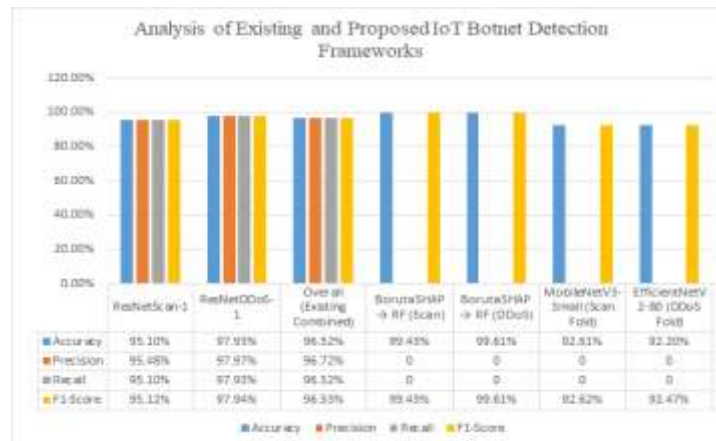


Figure 5 Comparative Performance Analysis of Existing and Proposed IoT Botnet Detection Frameworks

The above figure 5 presents a comparative analysis of the existing and proposed IoT botnet detection frameworks using Accuracy, Precision, Recall, and F1-score. The existing ResNet-18 models achieve strong performance with a combined accuracy of 96.52%, while the BorutaSHAP-based Random Forest models exceed 99% accuracy, demonstrating highly discriminative feature selection.

V. CONCLUSION

The proposed two-fold IoT botnet detection framework effectively addresses the challenges associated with multi-stage cyberattacks by enabling early scan detection and subsequent DDoS identification. By integrating BorutaSHAP-based feature selection with lightweight

deep learning architectures, namely MobileNetV3-Small and EfficientNetV2-B0, the framework achieves a balance between detection accuracy, computational efficiency, and model interpretability. Experimental evaluation using CICIDS2017, CICIDS2019, Bot-IoT, ScanLab, and DDoSLab datasets demonstrates the robustness and generalization capability of the proposed approach. The BorutaSHAP-based surrogate models achieved accuracies exceeding 99%, while the lightweight CNN models maintained competitive performance with reduced computational overhead. Furthermore, SHAP-based explainability enhanced transparency by providing insights into feature contributions. Future work will focus on real-time deployment in edge environments, federated learning integration, multiclass attack detection, and improving resilience against zero-day and adversarial attacks in large-scale IoT ecosystems.

References

- [1] Sagu, Amit, et al. "Scalable and Interpretable Deep Learning-Based Intrusion Detection Framework for Secure Internet of Things Networks." *Security and Privacy* 9.1 (2026): e70179.
- [2] Vishnu, Devraj, and Maheshwari Prasad Singh. "Hybrid multi-model ensemble framework for cybersecurity: threat detection and defense against assorted network intrusion attacks." *International Journal of Machine Learning and Cybernetics* 17.3 (2026): 119.
- [3] Saied, Mohamed, and Shawkat Guirguis. "Explainable artificial intelligence for botnet detection in internet of things." *Scientific Reports* 15.1 (2025): 7632.
- [4] Bobade, Sandip Y., et al. "Intelligent detection framework for IoT-botnet detection: DBN-RNN with improved feature set." *Journal of Information Security and Applications* 89 (2025): 103961.
- [5] Ashok Kumar, V., and G. R. Kanagachidambaresan. "Combined Deep Learning Framework With Selective Features for Botnet Attack Detection in Internet of Things." *Computational Intelligence* 41.6 (2025): e70157.
- [6] Sagu, Amit, et al. "Scalable and Interpretable Deep Learning-Based Intrusion Detection Framework for Secure Internet of Things Networks." *Security and Privacy* 9.1 (2026): e70179.
- [7] Badr, Nour Eldin Alaa, Xing Liang, and Jean-Christophe Nebel. "Improved Lightweight Cloud-Based Multiclass Cyber Intrusion Detection: Optimising FastViT with Boruta-SHAP and Class Balancing on CSE-CIC-IDS2018." 2025 6th International Conference on Computer Vision and Data Mining (ICCVDM). IEEE, 2025.
- [8] Vishnu, Devraj, and Maheshwari Prasad Singh. "Hybrid multi-model ensemble framework for cybersecurity: threat detection and defense against assorted network intrusion attacks." *International Journal of Machine Learning and Cybernetics* 17.3 (2026): 119.
- [9] EL ASRY, C. H. A. D. I. A. "Détection Avancée d’Intrusions par Machine Learning: Synergie entre Apprentissage Séquentiel, Sémantique et Représentation en Graphe." (2025).
- [10] Kalidindi, Archana, and Mahesh Babu Arrama. "Feature selection and hybrid CNNF deep stacked autoencoder for botnet attack detection in IoT." *Computers and Electrical Engineering* 122 (2025): 109984.



- [11] Hossain, Md Alamgir, and Md Samiul Islam. "Towards decentralized cybersecurity: a novel privacy-preserving federated learning approach for botnet attack detection." *Blockchain: Research and Applications* (2025): 100355.
- [12] Rupanetti, Dulana, and Naima Kaabouch. "Leveraging Machine Learning for Botnet Attack Detection in Edge-Computing Assisted IoT Networks." *arXiv preprint arXiv:2508.01542* (2025).
- [13] Wasswa, Hassan, Hussein A. Abbass, and Timothy Lynar. "Latent space alignment for robust detection of IoT botnet attacks in non-stationary environments." *Knowledge-Based Systems* (2025): 114749.
- [14] Polam, Ram Mohan, et al. "Advanced Machine Learning for Robust Botnet Attack Detection in Evolving Threat Landscapes." Available at SSRN 5515384 (2025).
- [15] Sheheryar, Mir Aman, and Sparsh Sharma. "Ensemble Feature Engineering and Deep Learning for Botnet Attacks Detection in the Internet of Things." *Transactions on Emerging Telecommunications Technologies* 36.3 (2025): e70099.
- [16] Bindu, Nalluri Venkata Madhu, et al. "IoT botnet detection from software defined network using American zebra optimization algorithm with SSRNN-ELM." *International journal of information technology* 17.2 (2025): 959-967.
- [17] Gelgi, Metehan, et al. "Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques." *Sensors* 24.11 (2024): 3571.
- [18] Alshaeaa, Hyder Yahya, and Zainab Mohammed Ghadhban. "Developing a hybrid feature selection method to detect botnet attacks in IoT devices." *Kuwait Journal of Science* 51.3 (2024): 100222.
- [19] De Vivo, Simona, et al. "DDoShield-IoT: a testbed for simulating and lightweight detection of IoT botnet DDoS attacks." 2024 54th annual IEEE/IFIP international conference on dependable systems and networks workshops (DSN-W). IEEE, 2024.
- [20] Alshaeaa, Hyder Yahya, and Zainab Mohammed Ghadhban. "Developing a hybrid feature selection method to detect botnet attacks in IoT devices." *Kuwait Journal of Science* 51.3 (2024): 100222.
- [21] Habibi, Omar, Mohammed Chemmakha, and Mohamed Lazaar. "Imbalanced tabular data modelization using CTGAN and machine learning to improve IoT Botnet attacks detection." *Engineering Applications of Artificial Intelligence* 118 (2023): 105669.
- [22] Habibi, Omar, Mohammed Chemmakha, and Mohamed Lazaar. "Imbalanced tabular data modelization using CTGAN and machine learning to improve IoT Botnet attacks detection." *Engineering Applications of Artificial Intelligence* 118 (2023): 105669.
- [23] Saif, Sohail, Nahal Yasmin, and Suparna Biswas. "Feature engineering based performance analysis of ML and DL algorithms for Botnet attack detection in IoMT." *International Journal of System Assurance Engineering and Management* 14.Suppl 1 (2023): 512-522.
- [24] Muñoz, David Concejal, and Antonio del-Corte Valiente. "A novel botnet attack detection for IoT networks based on communication graphs." *Cybersecurity* 6.1 (2023): 33.
- [25] Jakkani, Anil Kumar, Premkumar Reddy, and Jayesh Jhurani. "Design of a novel deep learning methodology for IoT botnet based attack detection." *International Journal on Recent and Innovation Trends in Computing and Communication* 11.9 (2023): 4922-4927.