A Stage-Wise, XAI-Driven Framework for Mirai Botnet Detection via Multi-Source Data Enrichment

Bishal Chhetry[1], Rajdeep Kumar Dutta[1], Rakesh Matam[1], Ferdous Ahmed Barbhuiya[1], Ashok Singh Sairam[2]
[1]Dept. of Computer Science and Engineering, Indian Institute of Information Technology Guwahati, India
[2]Dept. of Mathematics, Indian Institute of Technology Guwahati, India
Email: {bishal.chhetry, rajdeep.dutta, rakesh, ferdous}@iiitg.ac.in, ashok@iitg.ac.in

***Abstract*—The widespread use of the Internet of Things (IoT) ecosystem has introduced new vectors for sophisticated cyber-attacks. The Mirai botnet remains one of the most disruptive IoT threats, rapidly propagating across heterogeneous devices and launching high-volume Distributed Denial-of-Service (DDoS) attacks. Existing machine learning (ML) based intrusion detection systems (IDS) rely on public datasets such as IoT-23, CICIoT2023, and MedBIoT, but each captures only partial phases of Mirai's lifecycle (reconnaissance, exploitation, command-and-control (C&C) or DDoS). As a result, most detectors are tuned to identify late-stage DDoS traffic while offering limited visibility into early-stage activity, where intervention is most effective. This work constructs an enriched, stage-aligned dataset unifying IoT-23, CICIoT2023, and MedBIoT, mapping traffic flows to four Mirai phases: reconnaissance, exploitation, C&C communication, and attack execution. Using this dataset, We develop a stage-wise IDS based on Random Forest and XGBoost. Evaluated on a balanced dataset, the framework achieves 92% and 91% accuracy, respectively, across all stages. We further apply SHAP-based explainability to expose feature-level decision rationale for enabling actionable responses at the initial stage of an attack. Our results show that lifecycle-aware, interpretable detection enables proactive Mirai mitigation in real IoT environments.**

***Index Terms*—Internet of Things, Mirai, Distributed Denial-of-Service, Malware, Botnet Detection.**

I. Introduction

The Internet of Things (IoT) has transformed sectors such as healthcare, industrial automation, and smart homes by enabling seamless connectivity. However, this proliferation of resource-constrained devices has expanded the cyber-attack surface, exposing IoT networks to large-scale compromises [1]. Among these threats, the *Mirai* botnet [2] remains one of the most persistent and damaging, exploiting weak authentication to orchestrate massive Distributed Denial-of-Service (DDoS) campaigns, such as the 2016 Dyn attack [3] that disrupted major online services. These incidents underscore the need for proactive, interpretable, and scalable IoT defense mechanisms.

Existing *Mirai* detection research [4]–[7] relies primarily on public datasets like IoT-23 [8], CICIoT2023 [9], and MedBIoT [10]. Yet, these datasets capture only isolated portions of the attack lifecycle, limiting comprehensive detection. IoT-23, confined to three residential devices, lacks exploitation data; CICIoT2023 focuses on flooding attacks but omits Command-and-Control (C&C) communication; and MedBIoT includes propagation and C&C traffic but excludes reconnaissance and DDoS execution. Consequently, most IDS models identify Mirai only at its final stages, providing limited opportunity for early intervention.

Mirai progresses through five phases [11]: reconnaissance, exploitation, C&C communication, persistence, and attack execution (DDoS). Since the persistence stage leaves minimal network traces, it is excluded from this analysis. Detecting the earlier phases reconnaissance, exploitation, and C&C is critical for preempting large-scale attacks. However, most existing ML-based IDS lack such stage awareness and operate as opaque "black boxes", limiting trust and explainability. Recent advances in Explainable AI (XAI) [12] address this by revealing feature-level reasoning, enabling human analysts to interpret model outputs and act accordingly.

To bridge these gaps, this work introduces a **stage-wise, XAI-enabled Mirai detection framework** built on an **unified dataset** that consolidates IoT-23, CICIoT2023, and MedBIoT. The unified dataset provides balanced coverage across four key lifecycle stages reconnaissance, exploitation, C&C and attack execution. Using this dataset, we train lightweight Random Forest (RF) and XGBoost models optimized for IoT environments, integrating SHAP-based explanations to identify influential traffic features. This study therefore aims to build a transparent, lifecycle-aware detection model that enables early identification of Mirai's evolving behaviors across heterogeneous IoT environments.

A. Main Contributions

This paper makes the following contributions:

- **Comprehensive Lifecycle Dataset:** We construct an enriched dataset combining IoT-23, CICIoT2023, and MedBIoT, covering all major *Mirai* stages reconnaissance, exploitation, C&C, and attack execution thus eliminating stage coverage bias in existing datasets.
- **Explainable Stage-wise Detection:** We propose a Random Forest and XGBoost-based framework augmented with SHAP interpretability, providing transparent, actionable classification across all stages of the *Mirai* lifecycle.
- **Extensive Evaluation:** On a balanced dataset, our framework achieves 92% (RF) and 91% (XGBoost) accuracy, with SHAP analysis highlighting key flow features per stage for forensic insight and early mitigation.

Overall, this study establishes a lifecycle-aware, interpretable, and resource-efficient paradigm for IoT botnet de-

979-8-3315-7896-1/26/$31.00 ©2026 IEEE

tection, advancing the state of IoT security from reactive to proactive defense.

Organization: Section II reviews related work on IoT botnet detection, Section III details the enriched dataset and framework, Section IV presents experimental evaluation, and Section V concludes with future directions.

II. Related Work

The emergence of the *Mirai* botnet has motivated extensive research on intrusion detection mechanisms designed to mitigate IoT-based malware threats. Existing studies can be broadly classified into four categories: signature-based, anomaly-based, machine learning (ML)-based, and hybrid or reinforcement learning-based approaches.

Signature-Based Detection: These techniques [13] identify malicious activity by matching traffic patterns against known attack signatures. While these methods are effective for recognizing established *Mirai* variants, they fail to detect novel or obfuscated mutations, limiting adaptability in dynamic IoT environments.

Anomaly-Based Detection: Anomaly detection models [14] monitor deviations from normal system behavior to uncover unknown threats. Statistical approaches and biologically inspired models [15] have been explored, modeling traffic baselines to identify outliers. However, their high sensitivity to legitimate traffic variations results in excessive false positives, limiting scalability for large IoT deployments.

Machine Learning and Deep Learning Approaches: Recent advances employ data-driven methods to automate IoT threat identification. Li *et al.* [16] used CPU power fingerprinting and lightweight neural networks to detect *Mirai* variants with 99.10% accuracy, while Li *et al.* [17] utilized fine-grained side-channel features to identify zero-day malware, achieving 95.88% accuracy. Pham *et al.* [18] leveraged electromagnetic signals to detect obfuscated malware with 99.82% precision, highlighting the role of device-level signals in detection.

Traditional ML-based IDS models have also shown effectiveness in specific datasets. Studies using the IoT-POT dataset [5], [6] reported Random Forest (RF) and K-Nearest Neighbors (KNN) achieving near-perfect classification accuracy (up to 99.99%). Hybrid deep models further enhance temporal analysis capabilities: Alshehri *et al.* [19] proposed SkipGateNet, a CNN–LSTM model with learnable skip connections, reaching 99.91% accuracy and 8 ms inference time on the N-BaIoT dataset. Similarly, Kumar *et al.* [20] demonstrated LSTM's advantage in capturing sequential traffic dependencies for Mirai and Bashlite detection.

Reinforcement Learning and Hybrid Frameworks: Emerging techniques integrate reinforcement learning to adaptively enhance detection. Al-Fawa'reh *et al.* [4] introduced MalBoT-DRL, applying an attention-based reward function to improve feature selection, achieving 99.80% accuracy on MedBIoT and N-BaIoT. Gao *et al.* [21] proposed MACAE, a memory-assisted convolutional autoencoder that transformed traffic flows into spatial representations, achieving a low false alarm rate (FAR = 0.0511). Other hybrid studies combined temporal and spatial modeling: Kumari *et al.* [7] fused RNN and KNN for sequence-aware detection, while Palla *et al.* [22] compared ANN and RF classifiers, with ANN yielding 92.80% precision and an F1-score of 0.99.

Research Gaps and Motivation: While these studies demonstrate substantial progress in IoT malware detection through ML, DL, and DRL paradigms, several limitations persist. Most frameworks rely on isolated datasets such as IoT-23, MedBIoT, or CICIoT2023 [23], [24], each representing only partial stages of the *Mirai* attack lifecycle. Consequently, existing IDS models predominantly detect the later DDoS phase while overlooking early indicators such as reconnaissance, exploitation, and C&C communication. Furthermore, the black-box nature of deep models restricts interpretability and operational trust, particularly in safety-critical IoT environments.

To overcome these challenges, our work introduces a lifecycle-aware and explainable detection framework that unifies IoT-23, CICIoT2023, and MedBIoT into a comprehensive dataset representing all observable *Mirai* stages. Existing works overlook lifecycle completeness and model explainability, motivating the proposed stage-aware and XAI-enabled Mirai detection framework

III. Design and Methodology

Accurate Mirai detection requires datasets that comprehensively represent all stages of the attack lifecycle reconnaissance, exploitation, Command & Control (C&C) communication, and attack execution. Existing datasets such as IoT-23, CICIoT2023, and MedBIoT provide valuable insights but exhibit fragmented lifecycle coverage and limited diversity. To overcome these deficiencies, this study constructs a unified dataset that integrates samples across multiple stages, enabling holistic lifecycle representation and improved model generalization.

As illustrated in Fig. 1, the proposed framework comprises two primary stages. **Stage 1** focuses on dataset integration and enrichment, combining IoT-23, CICIoT2023, and MedBIoT to ensure end-to-end lifecycle coverage, including reconnaissance, exploitation, C&C, and DoS phases. **Stage 2** performs stage-wise model training using Random Forest and XGBoost classifiers. A SHAP-based explainability module interprets model predictions, enhancing transparency, trust, and operational applicability in real-world IoT defense.

TABLE I: Mirai Lifecycle Phase Coverage in Popular IoT Datasets

Dataset	**Scanning**	**Exploitation**	**C&C**	**DoS**
IoT-23 [8]	✓	✗	✓	✓
CICIoT2023 [9]	✓	✗	✗	✓
MedBIoT [10]	✗	✗	✓	✓
N-BaIoT [25]	✗	✓	✗	✓

A. Dataset Integration for Comprehensive Lifecycle Coverage

Table I summarizes the primary IoT datasets utilized in this study. Each dataset captures distinct segments of Mirai's

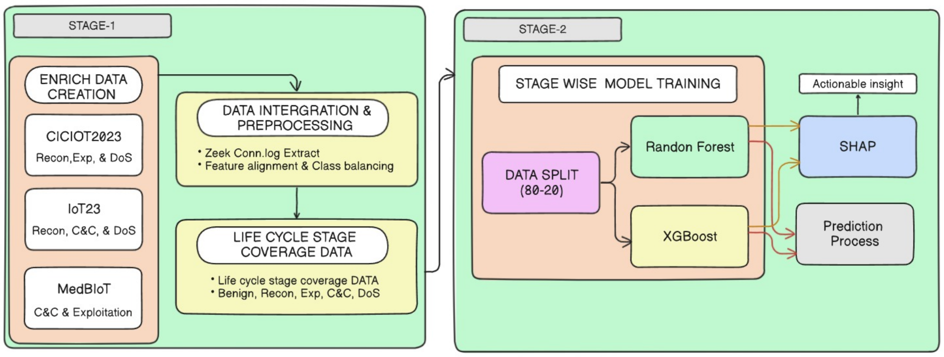


Fig. 1: Proposed two-stage framework for lifecycle-aware Mirai detection in IoT environments.

behavioral chain, contributing complementary insights across lifecycle phases. To achieve unified coverage, we merged and aligned relevant samples from IoT-23, CICIoT2023, and MedBIoT. Using the Zeek network analysis tool [26], [27], we extracted connection-level logs (`conn.log`) from packet captures to generate a consistent feature schema across datasets. This facilitated accurate labeling and mapping of samples to specific Mirai lifecycle stages.

Data Mapping to Lifecycle Stages:

- **Reconnaissance:** Derived from IoT-23 horizontal scan traces, capturing high-frequency connection attempts and IP probing activities.
- **Exploitation:** Brute-force authentication attempts from CICIoT2023, representing credential-based access compromise.
- **C&C Communication:** Incorporated from MedBIoT and IoT-23, including HeartBeat packets, command transmissions, and binary fetch operations.
- **Attack:** DDoS flows such as GREIP, GRETH, UDP, and TCP SYN floods from CICIoT2023 and IoT-23.
- **Benign:** Normal traffic from all three datasets, ensuring reliable model training and balanced evaluation.

B. Enhanced Lifecycle Representation and Generalization

The resulting unified dataset offers a balanced and comprehensive depiction of Mirai's network behavior across heterogeneous IoT environments. By merging datasets with varied device profiles and communication protocols, it mitigates dataset bias and strengthens cross-domain generalization. This consolidated dataset establishes a robust foundation for lifecycle-aware intrusion detection, capable of identifying early-stage threats before large-scale DDoS execution.

C. Framework for Multi-Stage Mirai Detection

With the dataset labeled according to Mirai's lifecycle stages Benign, Reconnaissance, Exploitation, C&C Communication, and DDoS. We developed a machine learning framework for stage-wise intrusion detection. RF and XGBoost were selected for their proven balance between accuracy, interpretability, and computational efficiency in IoT environments.

The framework follows three sequential steps:

Data Preprocessing: The merged dataset was cleaned, normalized, and feature-aligned to ensure uniformity across all data sources.

Model Training: RF and XGBoost classifiers were trained separately on stage-labeled samples to learn discriminative patterns corresponding to each phase of the Mirai lifecycle.

Evaluation: Models were assessed using accuracy, precision, recall, F1-score, and confusion matrices to evaluate both overall performance and stage-specific detection capability.

Leveraging lifecycle data and SHAP explainability, the framework achieves early, interpretable, and scalable Mirai detection in IoT networks.

IV. Results and Discussion

The proposed stage-wise detection framework was evaluated on the unified Mirai dataset described in Section III. The dataset was balanced to ensure equitable representation of all five categories Benign, Reconnaissance, Exploitation, C&C Communication, and Attack each containing 100,000 samples. This balance, yielding a total of 500,000 records, minimizes class bias and enables a fair comparison of model performance. The dataset was partitioned in an 80:20 ratio for training and testing, respectively.

A. Classification Performance

We evaluated the Random Forest (RF) and XGBoost classifiers using standard performance metrics: precision, recall, F1-score, accuracy, and Area Under the ROC Curve (AUC). The results in Tables II and III show that both models effectively distinguish Mirai lifecycle stages. RF achieved a slightly higher overall accuracy (92%) than XGBoost (91%) and better recall for C&C communication, suggesting improved sensitivity to subtle coordination patterns. Figures 2 and 3 illustrate that both models maintained AUC values near 1 across critical classes such as Attack and Exploitation, demonstrating excellent discriminatory power.

B. Confusion Matrix Analysis

Figures 4 and 5 present the confusion matrices for RF and XGBoost. Both models demonstrated strong performance

TABLE II: Classification Metrics for Random Forest

Class	Precision	Recall	F1-score
Attack	1.00	1.00	1.00
Benign	0.75	0.94	0.84
C&C Communication	0.92	0.68	0.78
Exploitation	0.99	1.00	1.00
Reconnaissance	0.99	0.99	0.99
Accuracy			**0.92%**

TABLE III: Classification Metrics for XGBoost

Class	Precision	Recall	F1-score
Attack	1.00	1.00	1.00
Benign	0.74	0.91	0.81
C&C Communication	0.87	0.66	0.75
Exploitation	0.99	1.00	0.99
Reconnaissance	0.98	0.98	0.98
Accuracy			**0.91%**

across all classes, though minor confusion occurred between Benign and C&C traffic due to overlapping temporal and packet-size characteristics. RF misclassified 6,163 benign samples as C&C, whereas XGBoost misclassified 6,331. This emphasizes the importance of interpretable models capable of highlighting overlapping traffic characteristics for deeper inspection. Overall, the models' consistent recognition of Exploitation and Reconnaissance stages confirms their suitability for early detection.

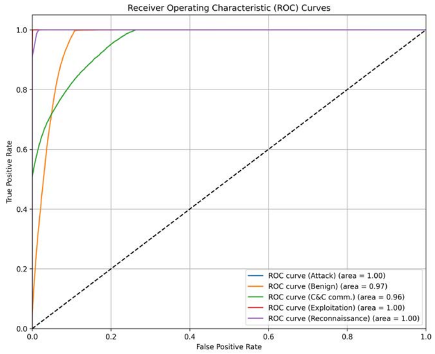


Fig. 2: ROC Curve for Random Forest.

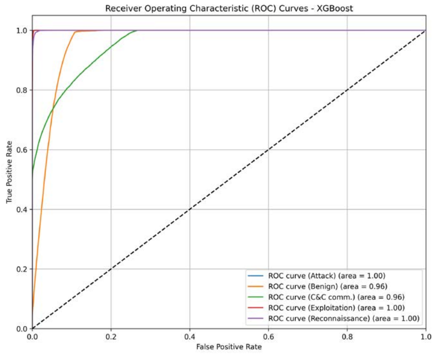


Fig. 3: ROC Curve for XGBoost.

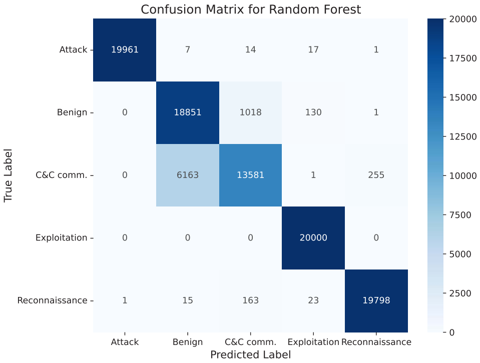


Fig. 4: Confusion Matrix for Random Forest.

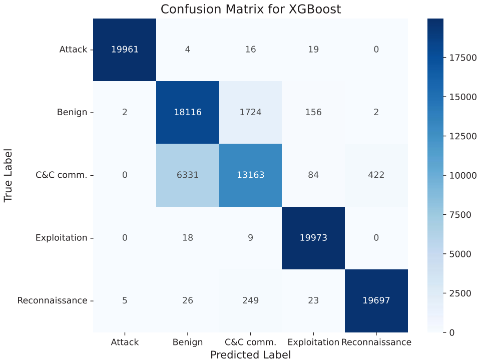


Fig. 5: Confusion Matrix for XGBoost.

C. Comparison with State-of-the-Art Methods

Table IV compares the proposed stage-wise framework with representative state-of-the-art (SOTA) Mirai detection approaches. While several deep learning models report higher accuracy on specific datasets, they typically concentrate on the final DDoS or C&C phases, neglecting early-stage behaviors essential for proactive mitigation. Most also function as opaque, non-interpretable systems.

As shown in Table IV, most prior works achieve superior accuracy by overfitting to narrow datasets or by focusing on high-volume attack traffic (DDoS). However, these models lack lifecycle diversity and interpretability. In contrast, our framework covers the entire Mirai progression from reconnaissance to attack enabling early detection and root-cause traceability. Although the achieved accuracy (91–92%) is marginally lower, the inclusion of multi-source data and XAI-driven explainability provides greater robustness, transparency, and operational relevance for real-world IoT defense. This balance between performance and interpretability marks a substantial improvement over traditional black-box IDS architectures.

D. Explainability and Feature Insights

Explainability is critical in operational security, where decisions must be interpretable and actionable. We employed SHAP values to interpret RF and XGBoost pre-

TABLE IV: Comparison of State-of-the-Art Mirai Detection Approaches with the Proposed Stage-wise Framework

No.	Works	Dataset(s)	Methodology	Lifecycle Coverage	Explainability	Accuracy (%)	Key Limitation
1	Alshehri *et al.* [19]	N-BaIoT	CNN–LSTM (SkipGateNet)	Attack only	✗	99.91	Focused on final DDoS stage; no early-stage insight
2	Kumar *et al.* [20]	IoT-POT	LSTM / RF / SVM	Attack only	✗	99.80	Sequential analysis only; ignores reconnaissance and C&C
3	Al-Fawa'reh *et al.* [4]	MedBIoT, N-BaIoT	DRL with attention reward	C&C, Attack	✗	99.80	Partial lifecycle coverage; black-box model
4	Gao *et al.* [21]	MedBIoT	CNN–Autoencoder (MACAE)	C&C, Attack	✗	97.06	Limited dataset; no feature interpretability
5	Li *et al.* [16]	Device-specific traces	Lightweight NN	Device anomaly	✗	99.10	Device-level only; not scalable
6	**Proposed Work**	IoT-23 + CICIoT2023 + MedBIoT	RF, XGBoost + SHAP (Stage-wise)	Recon, Exploit, C&C, Attack	**✓(SHAP)**	**92 - RF / 91 - XGBoost**	Slightly lower accuracy but full lifecycle and explainable detection

dictions across all Mirai lifecycle stages. Figures 6a–6e display the top contributing features per class. For the Attack phase, `conn_state_RSTOS0` (SHAP = 0.103) and `history` (0.072) were most indicative of anomalous sessions. In the Benign class, `duration` (0.073) and `source_ip_bytes` (0.064) dominated, reflecting stable communication patterns. C&C traffic exhibited persistence in `duration` and `source_ip_bytes`, while Exploitation was characterized by `local_source` (0.128) and `conn_state_S0`. Reconnaissance displayed long interaction durations (`duration`=0.126) and frequent probe attempts.

Comparative SHAP analysis reveals that RF provided clearer interpretability and higher recall for C&C traffic, whereas XGBoost captured subtler inter-feature correlations. Integrating SHAP thus enhanced transparency, enabling analysts to trace specific traffic attributes influencing classification. This interpretability not only strengthens model trustworthiness but also supports forensic analysis and real-time mitigation.

E. Discussion

While SOTA studies report accuracies nearing 99%, they primarily emphasize reactive detection of DDoS traffic. Our framework, though slightly lower in numerical accuracy, delivers a broader operational advantage: multi-dataset generalization, complete lifecycle visibility, and human-interpretable reasoning. These qualities make it better suited for deployment in heterogeneous IoT environments where explainability and early response outweigh marginal accuracy gains. Consequently, this stage-wise XAI-enabled model represents a shift from purely predictive IDS to *interpretable, context-aware defense systems* for IoT networks.

V. Conclusion

This study advances IoT security by addressing major gaps in Mirai botnet detection, especially the limited representation of early lifecycle stages. We introduced an enriched dataset, integrating IoT-23, CICIoT2023, and MedBIoT, providing comprehensive coverage from reconnaissance to attack execution. The proposed stage-wise framework, built on Random Forest and XGBoost classifiers, achieved high accuracy (92% and 91%) while providing SHAP-based interpretability that highlights the most influential features across each lifecycle stage. This explainability empowers proactive threat mitigation and bridges automated detection with human expertise. Future work will focus on integrating federated learning for privacy-preserving, distributed detection and on developing lightweight XAI modules optimized for resource-constrained IoT devices. Overall, this lifecycle-aware, interpretable framework transitions IoT intrusion detection from reactive response to proactive defense.

Acknowledgement: The authors acknowledge the support received from the Ministry of Electronics and Information Technology (MeitY), Government of India, through the project "LogIT: A Federated Learning and Fog-Computing based Framework for IoT Security" (Grant No. AAA-22/11/2022-CSD). This work has also been partially supported by ANRF, Government of India under the Grant ANRF/PAIR/2025/000010/PAIR.

References

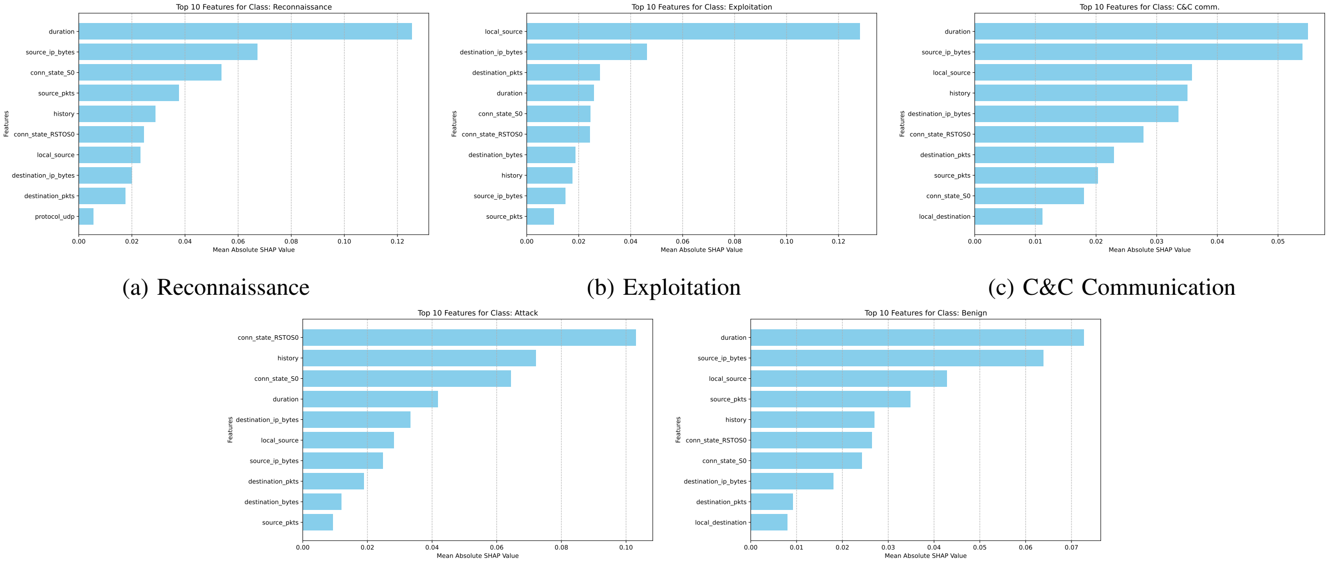
[1] T. Xu, J. B. Wendt, and M. Potkonjak, "Security of iot systems: Design challenges and opportunities," in *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 417–423, 2014.

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, (Vancouver, BC), pp. 1093–1110, USENIX Association, Aug. 2017.

[3] D. Dynamics, "Major ddos attack on dyn disrupts aws, twitter, spotify, and more," 2016. Accessed: 2025-01-15.

[4] M. Al-Fawa'reh, J. Abu-Khalaf, P. Szewczyk, and J. J. Kang, "Malbot-drl: Malware botnet detection using deep reinforcement learning in iot networks," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9610–9629, 2024.

[5] A. K. Jilani, F. Ahmad, M. A. R. Khan, and A. Jabeen, "Machine learning based framework for attack detection on iot devices," in *2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, pp. 1–8, 2023.



(a) Reconnaissance

(b) Exploitation

(c) C&C Communication

(d) Attack (DDoS)

(e) Benign

Fig. 6: SHAP Value Analysis Across Mirai Lifecycle Stages.

[6] A. Sharma and H. Babbar, "Iot-pot: Machine learning-based detection of mirai botnet attacks in iot," in *2024 First International Conference on Innovations in Communications, Electrical and Computer Engineering (ICICEC)*, pp. 1–6, 2024.

[7] A. Kumari, D. Gupta, and M. Uppal, "Unifying rnn and knn for enhancing mirai attack detection in iot networks," in *2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems (ICITEICS)*, pp. 1–5, 2024.

[8] S. Garcia, A. Parmisano, and M. J. Erquiaga, "IoT-23: A labeled dataset with malicious and benign IoT network traffic," 2020.

[9] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, 2023.

[10] A. Guerra-Manzanares, J. Medina-Galindo, H. Bahsi, and S. Nõmm, "MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network," in *Proceedings of the 6th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP*, pp. 207–218, SCITEPRESS, 2020.

[11] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, "The evolution of mirai botnet scans over a six-year period," *Journal of Information Security and Applications*, vol. 79, p. 103629, 2023.

[12] A. Oseni, N. Moustafa, G. Creech, N. Sohrabi, A. Strelzoff, Z. Tari, and I. Linkov, "An explainable deep learning framework for resilient intrusion detection in iot-enabled transportation networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 1, pp. 1000–1014, 2023.

[13] T. Al-Shurbaji, M. Anbar, S. Manickam, I. H. Hasbullah, N. ALfriehate, B. A. Alabsi, A. R. Alzighaibi, and H. Hashim, "Deep learning-based intrusion detection system for detecting iot botnet attacks: A review," *IEEE Access*, pp. 1–1, 2025.

[14] M.-L. Shyu, S. Chen, K. Sarinnapakorn, and L. Chang, "A novel anomaly detection scheme based on principal component classifier," 2003.

[15] P. Saurabh and B. Verma, "Negative selection in anomaly detection—a survey," *Comput. Sci. Rev.*, vol. 48, May 2023.

[16] Z. Li and D. Zhao, "Thingnet: a lightweight real-time mirai iot variants hunter through cpu power fingerprinting," in *Proceedings of the 2022 Conference & Exhibition on Design, Automation & Test in Europe*, DATE '22, (Leuven, BEL), p. 310–315, European Design and Automation Association, 2022.

[17] Z. Li and D. Zhao, "Zerod-fender: A resource-aware iot malware detection engine via fine-grained side-channel analysis," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 29, Oct. 2024.

[18] D.-P. Pham, D. Marion, M. Mastio, and A. Heuser, "Obfuscation revealed: Leveraging electromagnetic signals for obfuscated malware classification," in *Proceedings of the 37th Annual Computer Security Applications Conference*, ACSAC '21, (New York, NY, USA), p. 706–719, Association for Computing Machinery, 2021.

[19] M. S. Alshehri, J. Ahmad, S. Almakdi, M. A. Qathrady, Y. Y. Ghadi, and W. J. Buchanan, "Skipgatenet: A lightweight cnn-lstm hybrid model with learnable skip connections for efficient botnet attack detection in iot," *IEEE Access*, vol. 12, pp. 35521–35538, 2024.

[20] I. Kumar, M. Bohra, N. Mohd, and T. Singh, "Distributed denial of services (ddos) iot botnet malware identification using machine learning deep learning models," in *2024 Second International Conference on Advances in Information Technology (ICAIT)*, vol. 1, pp. 1–6, 2024.

[21] J. Gao, M. Fan, Y. He, D. Han, Y. Lu, and Y. Qiao, "Macae: memory module-assisted convolutional autoencoder for intrusion detection in iot networks: Macae: memory module-assisted convolutional autoencoder...," *J. Supercomput.*, vol. 81, Dec. 2024.

[22] T. G. Palla and S. Tayeb, "Intelligent mirai malware detection in iot devices," in *2021 IEEE World AI IoT Congress (AIIoT)*, pp. 0420–0426, 2021.

[23] A. K. Jilani, F. Ahmad, M. A. R. Khan, and A. Jabeen, "Machine learning based framework for attack detection on iot devices," *2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, pp. 1–8, 2023.

[24] A. G. Kumar, A. Rastogi, and V. Ranga, "Evaluation of different machine learning classifiers on new iot dataset ciciot2023," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, pp. 1–6, 2024.

[25] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.

[26] "Zeek: The network security monitor." https://zeek.org/get-zeek/. Accessed: 2025-01-17.

[27] V. Paxson, "Bro: A system for detecting network intruders in real-time," in *Proceedings of the 7th USENIX Security Symposium*, pp. 31–51, USENIX Association, 1999.