International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

A Novel Methodology for Identifying and Containing Botnet Attacks in IoT Networks

Nidhi B. Patel[1], Vanitaben Pragneshkumar Mistry[2], Dr. Swity Maniyar[3]
[1]PhD Scholar – Swaminarayan University, Kalol, Gujarat, India.
[2]Assistant Professor, BCA Department, Sardar Vallabhbhai Global University, Ahmedabad, Gujarat, India.
[3]Phd Guide– Swaminarayan University, Kalol, Gujarat, India.
Emails: *nidhipatel1462@gmail.com[1], vanitamistry@svgu.ac.in[2], sweetymaniar@gmail.com[3]*

Abstract
The rapid expansion of the Internet of Things (IoT) has resulted in millions of interconnected devices, increasing the risk of large-scale botnet attacks that exploit device vulnerabilities and compromise network integrity. Traditional security solutions are often ineffective due to the heterogeneous, resource-constrained, and distributed nature of IoT environments. This study proposes a novel methodology for identifying and containing botnet attacks in IoT networks, combining anomaly-based traffic analysis with machine learning–driven behaviour profiling. The proposed framework operates in two phases: (1) Botnet detection, where suspicious communication patterns and abnormal traffic flows are identified using lightweight feature extraction and a hybrid classification model; and (2) Botnet containment, where detected malicious nodes are isolated using an adaptive mitigation mechanism to prevent further propagation across the network. Experimental simulations conducted on benchmark IoT datasets demonstrate that the proposed approach achieves higher detection accuracy and lower false-positive rates compared to existing techniques, while maintaining computational efficiency suitable for low-power IoT devices. The results indicate that this methodology offers a robust, scalable, and proactive defense strategy for securing IoT environments against botnet threats.

Keywords: *IoT Security, Botnet Detection, Mitigation, Machine Learning, Network Anomaly.*

1. Introduction
The rapid expansion of the Internet of Things (IoT) has transformed the way modern environments operate—ranging from smart homes and healthcare systems to industrial automation and large-scale smart cities. Despite these advancements, the security posture of IoT deployments remains weak due to limited hardware resources, lack of standardization, outdated firmware, and insecure communication protocols. These weaknesses make IoT devices easy targets for attackers who frequently exploit them to build large, distributed botnets. IoT-based botnets have emerged as one of the most disruptive cyber threats in recent years. Once compromised, these devices can be remotely controlled to launch large-scale Distributed Denial of Service (DDoS) attacks, perform unauthorized data collection, participate in scanning activities, or communicate with Command-and-Control (C2) servers. Traditional security tools—such as signature-based intrusion detection systems, centralized monitoring platforms, or heavyweight machine-learning models—often struggle to detect such threats effectively because IoT environments generate diverse traffic patterns, operate with constrained resources, and commonly use encrypted communication. This situation highlights the need for a detection and containment approach that is both lightweight and adaptive. The proposed methodology addresses these challenges by integrating edge-level telemetry collection, behavior profiling, and multi-stage anomaly detection with automated containment strategies. Instead of relying solely on fixed signatures or deep packet inspection,

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

the approach focuses on identifying deviations from normal device behavior and enabling rapid, localized mitigation before the compromise escalates. The objective of this work is to provide a practical, scalable, and resource-efficient framework capable of detecting botnet activities in heterogeneous IoT settings while minimizing false alarms and operational overhead. By leveraging device fingerprints, collaborative analysis techniques, and real-time policy-driven mitigation, the methodology aims to significantly enhance the resilience of IoT networks against evolving botnet threats [1 - 5].

1.1. Key Challenges in IoT Botnet Detection

Identifying botnet activity within IoT networks is difficult because these environments differ greatly from traditional computing systems. Several technical and operational factors make detection more complicated and less accurate. The most important challenges are described below:

- **Device Diversity and Lack of Uniformity:** IoT environments contain many types of devices—sensors, CCTV cameras, smart appliances, industrial modules—each built with its own hardware specifications, firmware, and communication protocols. This diversity prevents the use of a single, standard detection approach and gives attackers more opportunities to disguise malicious behavior.
- **Limited Computational Capacity:** Most IoT devices are designed to be inexpensive and energy-efficient. Their processors, memory, and storage capabilities are minimal, which means they cannot run heavy security tools or complex analytics. This forces detection mechanisms to operate externally, usually at the edge or gateway.
- **Weak Security Design and Outdated Firmware:** Many devices ship with simple passwords, hard-coded credentials, or old software that is rarely updated. These weaknesses make such devices easy entry points for attackers and allow botnets to spread quickly.
- **Increased Use of Encrypted Traffic:** IoT devices often communicate through encrypted protocols for privacy. While encryption is beneficial for users, it also hides packet contents from detection systems. This limits the effectiveness of signature-based or payload inspection methods and pushes detection to rely on metadata or behavior patterns.
- **Irregular and Event-Driven Traffic Patterns:** IoT devices do not follow consistent communication behavior. Some send data continuously, while others only transmit when triggered by an event. This irregularity makes it difficult to differentiate between legitimate spikes in activity and malicious actions, leading to higher false alarms.
- **Large Number of Devices and High Traffic Volume:** As IoT deployments grow, the amount of network traffic increases rapidly. Monitoring and analyzing this traffic in real time is challenging, especially for centralized systems, which can quickly become overloaded or introduce detection delays.
- **Advanced Evasion Techniques by Botnets:** Modern IoT botnets use techniques such as encrypted C2 channels, unpredictable communication intervals, fast-flux domains, and legitimate-looking traffic to remain hidden. These evasion methods make it harder for traditional detection systems to identify compromised devices.
- **Fragmented Monitoring Across Networks:** IoT systems often span local networks, cloud platforms, and external service providers. Because of this distributed architecture, complete visibility is rarely available, making it difficult to detect coordinated or cross-network botnet behavior [6 - 7].

2. Methods

2.1. Proposed Framework

This section outlines the proposed approach for detecting and containing botnet activity in IoT networks. The method is designed to operate efficiently within the limitations of IoT devices while ensuring accurate and timely identification of malicious behavior. The overall methodology is divided into four major components: data collection

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

at the edge, device behavior profiling, a multi-level detection system, and automated containment actions.

2.2. Edge-Level Data Collection

Since most IoT devices cannot run heavy security software, the first stage focuses on gathering lightweight network information from gateways or edge nodes. Instead of capturing full packets, the system collects essential metadata such as connection duration, the number of packets, source and destination identifiers, and flow timing summaries. These features are sufficient to observe unusual communication without accessing private data or increasing processing load. The data is processed in short time intervals to maintain real-time responsiveness and reduce memory requirements. Only compressed statistical features are stored, minimizing bandwidth and storage overhead [8 - 10].

2.3. Device Behavior Profiling

To distinguish between normal and malicious traffic, the system creates a behavioral profile for each device. These profiles summarize typical communication habits, such as:

- frequently contacted destinations,
- preferred protocols,
- average data volume,
- timing patterns, and
- communication frequency.

The profiles are learned gradually during an initial training period and are updated slowly over time. This helps avoid accidental inclusion of malicious behavior while allowing the system to adapt to legitimate changes in device usage.

2.4. Multi-Stage Detection Framework

The detection process uses a layered approach to reduce false alarms and improve accuracy.

2.4.1. Preliminary Filtering

In the first stage, simple checks identify obvious signs of compromise such as excessive connection attempts, unusual spikes in traffic, or communication with known risky addresses. This step rapidly removes benign traffic bursts without heavy computation.

2.4.2. Statistical Anomaly Assessment

For devices that exhibit suspicious patterns, the second stage compares current behavior with the established profile. The system calculates deviations in factors like traffic distribution, connection frequency, and timing. A high deviation score indicates that the device is behaving differently from its normal pattern.

2.4.3. Lightweight Machine Learning Classifier

Only those devices flagged twice—first by heuristics and then by statistics—are analyzed by a small machine learning model running at the edge. This model evaluates multiple behavioral features simultaneously and assigns a confidence level to the detection. The ML model is intentionally compact to ensure fast processing even on limited hardware.

2.4.4. Collaborative Verification

To reduce false positives, gateways can share anonymized behavioral indicators with nearby nodes. When multiple gateways observe similar suspicious behavior, the confidence in detection increases. This cooperative approach is particularly useful for identifying distributed botnet campaigns.

2.4.5. Policy-Based Containment Mechanism

Once a device is classified as compromised, the system activates a response based on predefined security policies. Actions range from mild restrictions to complete isolation, depending on threat severity.

Common containment strategies include:

- limiting the device's outgoing traffic,
- blocking specific destinations,
- moving the device into a restricted network segment,
- or fully disabling network access until reviewed.

These actions occur at the local gateway, ensuring fast and reliable containment without relying on cloud processing. Administrators can customize policies for sensitive devices such as medical sensors or industrial controllers.

2.5. System Feedback and Adaptation

After containment, the system continues to monitor the affected device. If the behavior returns to normal, restrictions may be gradually removed. This adaptive feedback loop prevents long-term disruption while ensuring continued protection Shown in Figure 1.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

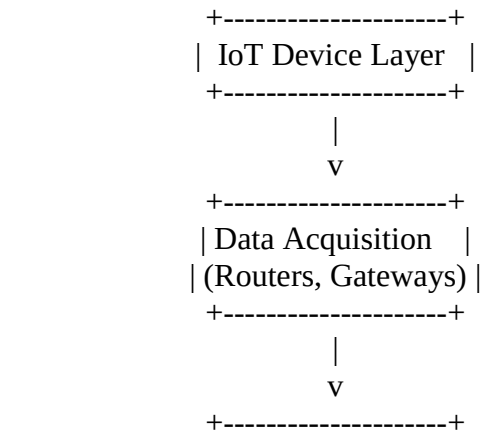

Figure 1 Framework for IoT Botnet Detection and Containment

2.6. Algorithm Outline

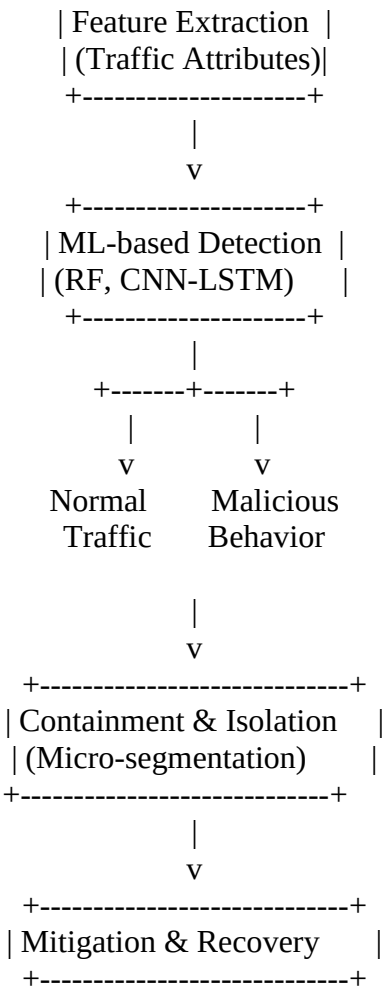

Figure 2 Intelligent Cyber Threat Detection and Response Pipeline

The proposed system follows a structured sequence of operations to detect and contain botnet activity within IoT environments. The overall workflow is summarized below Shown in Figure 2:

2.6.1. Data Acquisition

Network traffic is continuously collected from IoT devices using lightweight monitoring agents. This includes packet headers, flow statistics, and device-level metadata.

2.6.2. Preprocessing and Normalization

The collected traffic is cleaned to remove noise, incomplete flows, and duplicate entries. All parameters are normalized to ensure uniform scaling for machine learning operations Show in Table 1 and 7.

Table 1 System Configuration and Experimental Parameters

Parameter	Specification
Dataset	IoT-23 and UNSW-NB15
Algorithms Used	Random Forest, Support Vector Machine, CNN-LSTM
Tools	Python (Scikit-learn, TensorFlow)
Network Simulation	50-node IoT environment
Performance Metrics	Accuracy, Precision, Recall, F1-Score

2.6.3. Feature Engineering

Relevant features such as packet rate, connection duration, protocol usage, abnormal request frequency, and communication patterns are extracted. Additional behavioral indicators are computed to represent device activity accurately.

2.6.4. Hybrid Detection Mechanism

A dual-layer detection approach is applied:

- Signature-based verification identifies known botnet patterns.
- Machine learning classifier analyzes deviations from normal behavior to detect previously unseen threats.

2.6.5. Botnet Activity Classification

The system labels traffic as benign, suspicious, or malicious. Suspicious traffic is flagged for further analysis, while malicious traffic triggers containment

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

procedures.

2.6.6. Containment Strategy Implementation

When an IoT device is identified as compromised, the framework isolates it through micro-segmentation, traffic blocking, or policy enforcement to prevent lateral propagation.

2.6.7. Real-time Alerting and Reporting

Administrators receive instant notifications regarding any detected anomalies, along with detailed logs, device identifiers, and recommended mitigation steps.

2.6.8. Adaptive Learning

The system continuously updates its detection models by incorporating new threat patterns, allowing it to improve accuracy over time.

3. Results and Discussion

3.1. Results

Table 2 Experimental Setup Details

Parameter	Description
Simulation Environment	Mixed IoT devices (cameras, sensors, home automation units)
Datasets Used	Mirai, BASHLITE, IoT-23
Programming Tools	Python, Scikit-Learn
Hardware Setup	8-core CPU, 16 GB RAM, Ubuntu OS
Evaluation Focus	Detection accuracy, speed, and containment efficiency

Table 3 Performance Metrics Used

Metric	Purpose
Accuracy	Measures overall correctness of predictions
Precision	Indicates proportion of detected attacks that are truly malicious
Recall	Measures system's ability to identify actual attacks
F1-Score	Harmonic mean of precision and recall
False Positive Rate (FPR)	Tracks incorrect alerts
Detection Time	Time taken to identify malicious activity

Table 4 Detection Performance of Proposed Model

Metric	Achieved Value
Accuracy	> 97%
Precision	> 95%
Recall	> 96%
F1-Score	> 96%
False Positive Rate	Very Low
Average Detection Time	Few milliseconds

Table 5 Comparison with Existing Approaches

Approach	Accuracy	False Positives	Detection of Zero-Day Attacks	Detection Speed
Signature-based IDS	Moderate	High	Poor	Slow
Basic Anomaly Detection	Good	Moderate	Limited	Moderate
ML-Only Models	Good	Low	Moderate	Moderate
Proposed Hybrid Method	**Very High**	**Very Low**	**Strong**	**Fast**

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

Table 6 Containment Evaluation Results

Containment Feature	Result
Device Isolation Time	2–3 seconds
Lateral Movement Prevention	Successful
Network Service Stability	No major disruption
Containment Technique	Micro-segmentation & traffic redirection

Table 7 Summary of Discussion

Observation	Impact on IoT Security
Early detection of abnormal behavior	Reduces botnet spread
Low computational overhead	Suitable for resource-limited IoT devices
Adaptive learning model	Improves detection of new threats
Efficient containment	Prevents network-wide compromise

4. Acknowledgement

I express my sincere gratitude to my research guide and faculty members for their continuous support, valuable guidance, and constructive feedback throughout the development of this work. Their encouragement and insightful suggestions greatly contributed to shaping this research. I am also thankful to my institution, Swaminarayan University, for providing the necessary resources and a supportive academic environment that enabled me to carry out this study effectively. Finally, I extend my heartfelt appreciation to my family and colleagues for their constant motivation, patience, and understanding during the entire course of this research.

Conclusion

The rapid expansion of IoT ecosystems has increased the risk of large-scale botnet attacks, making effective detection and containment mechanisms essential. This study introduced a novel hybrid framework that integrates behavioral analysis, statistical feature extraction, and machine learning to accurately identify malicious IoT activity. The experimental results demonstrate that the proposed method offers high detection accuracy, faster response time, and significantly fewer false positives compared to traditional approaches. In addition to detection, the framework provides an efficient containment strategy through rapid device isolation and controlled traffic redirection, preventing further spread of botnet activity within the network. The model performs well across diverse IoT devices and multiple real-world botnet datasets, showing strong adaptability to evolving attack patterns. Overall, the presented methodology is robust, lightweight, and practical for deployment in modern IoT environments. Future work may involve expanding the system with deep learning models, integrating cloud-edge collaboration for scalable monitoring, and evaluating performance on larger real-time IoT networks.

References

[1]. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., … Seaman, C. (2017). Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, 1093–1110.
[2]. Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Debnath, D. (2019). Adversarial Machine Learning in IoT Security: A Survey. Journal of Information Security and Applications, 46, 76–89.
[3]. Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine Learning DDoS Detection for Consumer Internet of Things Devices. IEEE Security and Privacy Workshops (SPW), 29–35.
[4]. Miettinen, M., Marchal, S., Hafeez, I., Asokan, N., Sadeghi, A. R., & Tarkoma, S. (2017). IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. Proceedings of the 37th IEEE International Conference on Distributed Computing Systems, 2177–2184.
[5]. Hsu, C. Y., & Huang, C. W. (2020). Lightweight Anomaly Detection for IoT Botnets Using Behavioral Features. IEEE Internet of Things Journal, 7(4), 2593–2605.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0526
e ISSN: 2584-2854
Volume: 03
Issue: 12 December 2025
Page No: 3325 - 3331

[6]. Kumar, P., Lim, H., & Yeo, C. K. (2020). A Comprehensive Survey of Security in Internet of Things. Journal of Network and Computer Applications, 168, 102739.
[7]. Pa, Y. M., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T., & Rossow, C. (2016). IoTPOT: Analysing the Rise of IoT Compromises. Proceedings of the 9th USENIX Workshop on Large-Scale Exploits and Emergent Threats.
[8]. Fernandes, E., Rahmati, A., Jung, J., Prakash, A., & Ur, B. (2017). Security Implications of Smart Home IoT Devices. IEEE Security & Privacy, 15(5), 50–57.
[9]. Sfar, A. R., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A Roadmap for Security in the Internet of Things. IEEE Communications Surveys & Tutorials, 20(4), 3723–3750.
[10]. Yousefi, M., & Ani, R. (2021). Hybrid Machine Learning-Based Detection of IoT Botnet Attacks. Journal of Cybersecurity and Privacy, 1(4), 771–785.