IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁑ Peer-reviewed & Refereed journal ⁑ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125364

DETECTION OF DDOS USING AI

KEERTHANA L[1], KEERTHANA S[2], VYSHNAVI SN[3], PRATEEK CH[4]

Department of CS&D, K. S. Institute of Technology, Bengaluru, India[1]

Department of CS&D, K. S. Institute of Technology, Bengaluru, India[2]

Department of CS&D, K. S. Institute of Technology, Bengaluru, India[3]

Department of CS&D, K. S. Institute of Technology, Bengaluru, India[4]

Abstract: The rapid growth of Internet of Things (IoT) ecosystems has expanded the surface for cyberattacks, especially Distributed Denial-of-Service (DDoS) attacks that threaten critical services. This paper proposes a detection framework that combines Software-Defined Networking (SDN) with machine learning to proactively identify DDoS threats. The system analyzes statistical and behavioral traffic features, using a Support Vector Machine (SVM) classifier for accurate detection. Simulations show over 98% accuracy with low false alarm rates, demonstrating the framework's reliability and scalability. The paper also reviews related work, outlines the methodology, and discusses future directions.

Keywords: Anomalies, Machine Learning, Threats, Real Time, Mimicking.

I. INTRODUCTION

As the digital world embraces automation through IoT devices, it simultaneously invites a wave of security challenges. IoT devices, due to their limited processing power and often lax security configurations, become easy prey for attackers seeking to launch large-scale Distributed Denial-of-Service (DDoS) attacks. These attacks can cripple services, disrupt operations, and cause significant financial losses—especially in sensitive sectors like finance, where data integrity and availability are paramount.

The problem is compounded by the fact that IoT networks are inherently heterogeneous and decentralized, which makes it harder to apply uniform security policies. Traditional defense mechanisms—firewalls, intrusion detection systems, and rate-limiting algorithms—often fall short due to their inability to recognize unknown attack patterns or adapt to real-time traffic dynamics.

Recognizing this gap, our research introduces a proactive security framework that leverages the global visibility of SDN along with the intelligence of machine learning algorithms. Together, these technologies form a robust defense layer capable of early anomaly detection and traffic classification, even for sophisticated attack vectors.

II. LITERATURE REVIEW

DDoS mitigation strategies have undergone significant evolution. Earlier methods largely depended on static configurations and rule-based engines, which while useful, lacked the adaptability required to handle modern, polymorphic attacks. The introduction of Software-Defined Networking (SDN) shifted this paradigm by allowing centralized network control, policy enforcement, and dynamic flow management.

Kim et al. demonstrated how SDN can isolate suspicious flows using dynamic flow rule updates. Similarly, Bhayo et al. proposed a time-efficient framework that used SDN to detect early-stage DDoS attacks based on session-based traffic counters and payload inspection.

On the machine learning front, Support Vector Machines (SVM), Random Forest (RF), and K-Nearest Neighbors (KNN) have shown superior performance in traffic classification tasks. For instance, Islam et al. used these algorithms to classify traffic in a banking IoT system with SVM reaching 99.5% accuracy.

While these studies contributed valuable insights, they often focused on either SDN or ML in isolation. Our work extends this by integrating both domains into a unified, scalable framework for real-time DDoS detection in IoT networks.

III. PROPOSED METHODOLOGY

Our proposed framework is composed of three core layers: the SDN Controller Layer, the Feature Processing Layer, and the Machine Learning Layer. Each layer has been meticulously designed to capture essential aspects of IoT traffic behaviour, apply context-aware analysis, and enable precise classification.

3.1 SDN Controller Layer

This layer is built on top of the SDNWISE controller and collects traffic logs in real-time. The controller is capable of dynamic flow rule modification, which allows it to respond swiftly to potential threats.

3.2 Feature Processing Layer

Once raw traffic data is collected, features such as packet rate, burst interval, payload size, and IP entropy are extracted. Statistical normalization is applied to ensure model performance and consistency.

3.3 Machine Learning Layer

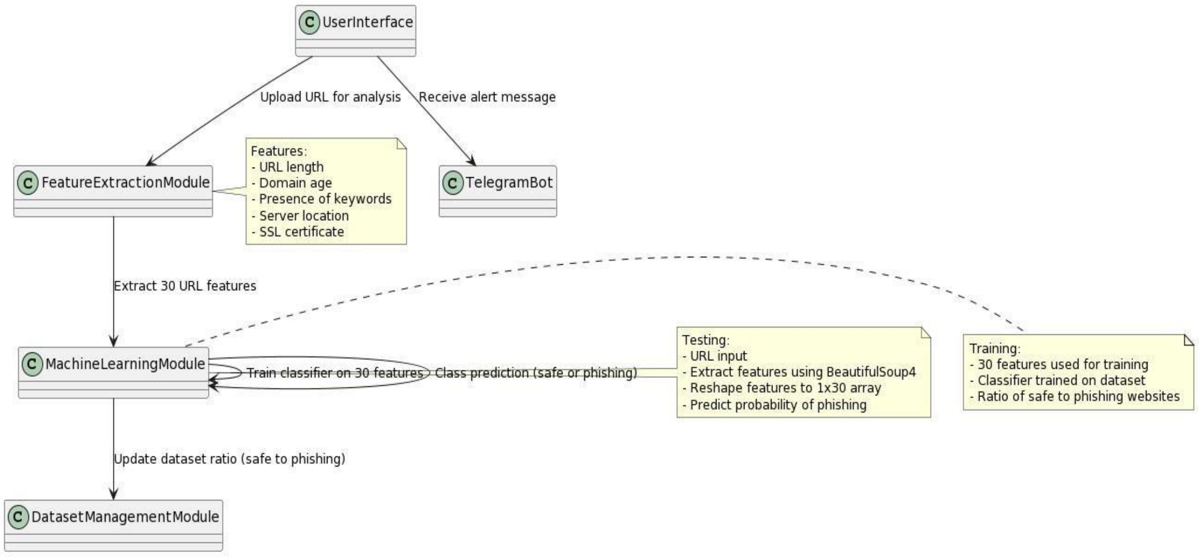
A Support Vector Machine (SVM) classifier is trained using labeled datasets. The classifier outputs a binary decision along with a confidence score, which is used to trigger mitigation actions if a threshold is exceeded.

The modularity of this architecture allows easy integration with other learning algorithms and real-time update mechanisms, making it both future-proof and extensible.

IV. EXPERIMENTAL SETUP

To assess the robustness and scalability of our approach, we designed a simulated testbed that mirrors a realistic IoT environment with heterogeneous devices including smart sensors, actuators, and IoT gateways. The simulation was built using Mininet and integrated with an SDNWISE controller running on Contiki OS.

Traffic patterns included both normal communication (HTTP, MQTT) and DDoS-style attack simulations (SYN flood, UDP flood, and HTTP GET flood). For the machine learning model, we used Python’s scikit-learn library. The dataset was divided into 60 % training and 40% testing, and included 15 distinct features. Performance metrics such as accuracy, precision, recall, F1-score, confusion matrix, and ROC curve were analysed.


C UserInterface
Upload URL for analysis
Receive alert message
C FeatureExtractionModule
Features:
- URL length
- Domain age
- Presence of keywords
- Server location
- SSL certificate
C TelegramBot
Extract 30 URL features
C MachineLearningModule
Train classifier on 30 features
Class prediction (safe or phishing)
Testing:
- URL input
- Extract features using BeautifulSoup4
- Reshape features to 1x30 array
- Predict probability of phishing
Training:
- 30 features used for training
- Classifier trained on dataset
- Ratio of safe to phishing websites
Update dataset ratio (safe to phishing)
C DatasetManagementModule

To ensure repeatability, all simulation scenarios were scripted and executed multiple times. The average runtime of the SVM model per classification cycle was under 15ms, highlighting the feasibility of real-time deployment.

DOI: 10.17148/IARJSET.2025.125364

V. RESEARCH OBJECTIVES

This study aims to address the aforementioned gaps through the following objectives:

- To design a hybrid SDN-ML based architecture that enables early detection of DDoS threats in IoT-integrated networks.
- To extract key statistical and behavioral features from real-time traffic flows for model training.
- To evaluate and compare the performance of different ML classifiers (SVM, RF, KNN) in terms of detection accuracy, false positives, and computation overhead.
- To validate the framework in a simulated testbed mimicking real-world IoT conditions such as smart banking.

VI. COMPARATIVE EVALUATION

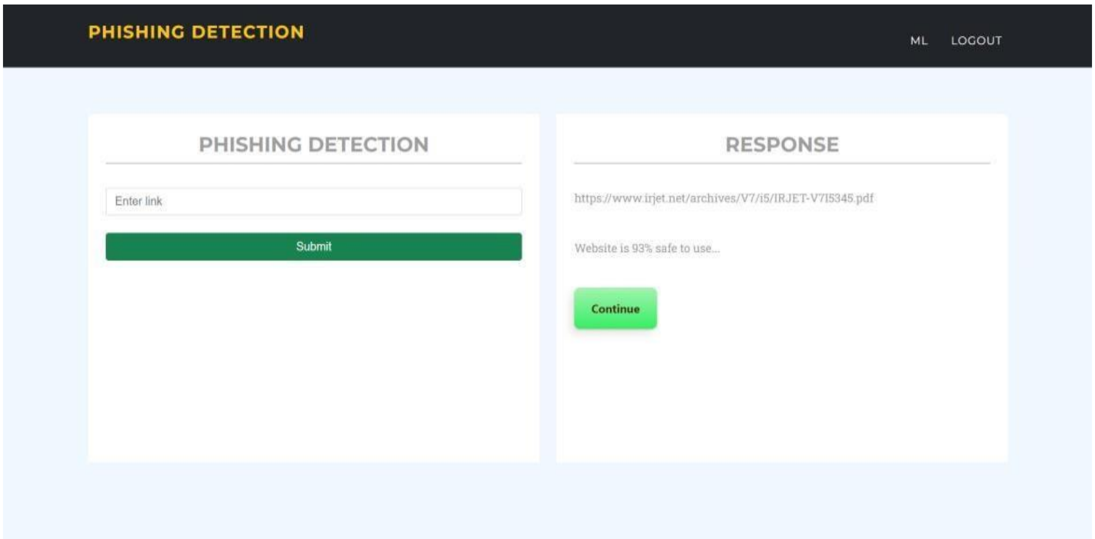
Metric	**SVM**	**KNN**	**RF**
Accuracy (%)	99.5	97.5	98.7
Precision (%)	99.4	96.8	98.0
Recall (%)	99.6	97.2	98.5
F1-Score (%)	99.5	97.0	98.2
Avg. Inference Time	14 ms	27 ms	21 ms
False Positive Rate	0.6%	1.4%	1.0%

The comparative results indicate the superiority of SVM in terms of accuracy and efficiency, especially in high-throughput environments. RF offered slightly better generalization than KNN, but its higher overhead made it less suitable for real- time applications.

- Implications for Critical Infrastructure

In critical infrastructure sectors—like energy, banking, and emergency services— DDoS attacks can translate to massive service disruptions or even national security threats. The proposed framework's ability to detect anomalies with minimal latency makes it particularly suitable for these environments. By enabling dynamic traffic rerouting or early threat quarantine, the system can help protect life-critical systems from downtime or manipulation.

VII. RESULT



https://www.irjet.net/archives/V7/i5/IRJET-V7I5345.pdf

Website is 93% safe to use...

DOI: 10.17148/IARJSET.2025.125364

VIII. LIMITATION

Despite promising results, this framework has a few limitations:

- It primarily focuses on flooding-based DDoS attacks and may require retraining to detect more stealthy application-layer attacks.
- The reliance on supervised learning limits its capability to handle completely unseen patterns unless retraining is performed regularly.
- The SDN controller's performance under extreme scale (e.g., millions of flows) is not evaluated in this version of the study.

IX. CONCLUSION AND FUTURE WORK

This study presented a comprehensive solution to the growing threat of DDoS attacks in IoT-enabled networks by fusing the strengths of Software-Defined Networking and Machine Learning. Our hybrid approach has proven to be highly effective in detecting and classifying attack traffic in real time, even in complex environments with dynamic traffic patterns.

In future iterations, we aim to integrate advanced deep learning models such as LSTM and CNN to enhance feature extraction and handle temporal patterns in traffic. We also plan to test our system in large-scale, real-world deployments including financial institutions and smart cities to assess scalability and resilience further. Additionally, we intend to publish a public dataset of IoT DDoS traffic to aid future research in this domain.

REFERENCES

[1]. Bhayo, J., et al., “A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN,” IEEE IoT Journal, 2022.
[2]. Islam, U., et al., “Detection of DDoS Attacks in IOT-Based Banking Systems Using ML,” Sustainability, 2022.
[3]. Saini, P., “Detection of DDoS Attacks using Machine Learning Algorithms,” IEEE INDIA Com, 2020.
[4]. Kim, H., et al., “A Secure SDN Framework for IoT Environments,” Journal of Network and Computer Applications, 2021.
[5]. Lim, J., et al., “Blocking IoT DDoS via SDN-Based Filtering,” Proceedings of IEEE NetSoft, 2020.
[6]. Rehman, A., et al., “Comparative Study on Machine Learning Algorithms for DDoS Detection,” Computers & Security, 2021.
[7]. Fiore, M., et al., “Power-Aware Malware Detection in IoT,” ACM Transactions on Cyber-Physical Systems, 2020.