

Real-Time Detection and Prevention of IOT-Based DDOS Attacks in Network Environments

Briggs, Toala Dimabo¹, Sako, D. J. S², Nwiabu, N. D³

Department of Computer Science,

Rivers State University, Port Harcourt, Nigeria

¹Briggs.toala@rsu.edu.ng, ²dum.sako@ust.edu.ng,

³nwiabu.nuka@ust.edu.ng

<https://doi.org/10.56201/ijasmt.vol.12.no9.2026pg24.33>

Abstract

The rapid growth of Inter-of-Things (IoT) devices and their weak security configurations have significantly increased the vulnerability of modern network infrastructures to different forms of sophisticated cyber-attacks, particularly low-rate, stealthy, and botnet-driven DDoS attacks. Existing traditional intrusion detection and prevention systems often suffer from high latency, poor adaptability to evolving attack patterns, inadequate real-time response mechanisms, and limited privacy-preserving capabilities. Therefore, to address these limitations, this paper presents a real-time intelligent framework for the analysis, detection, and prevention of IoT-based Distributed Denial of Service (DDoS) attacks in network environments. The developed system utilized Long Short-Term Memory (LSTM) as the core real-time detection engine for identifying malicious IoT traffic patterns based on temporal and behavioral network features, and Reinforcement Learning (RL) technique to design an intelligent automated prevention and response mechanism capable of mitigating malicious traffic patterns dynamically. Furthermore, Homomorphic Encryption (HE) using the Cheon-Kim-Kim-Song (CKKS) scheme was integrated into the framework to preserve the privacy of sensitive network traffic during storage, analysis and transmission. The system was implemented using Python programming language, while MongoDB served as the NoSQL database for data storage and management. Experimental results showed that the proposed system achieved an excellent detection and prevention performance, recording a detection accuracy of 98.3%, precision of 97.8%, recall of 98.6%, and F1-score of 98.2%. Similarly, the reinforcement learning prevention module achieved an attack-blocking accuracy of 99.2% with a low false positive rate of 0.8%, confirming its effectiveness in dynamically mitigating malicious traffic while allowing legitimate network communications to proceed uninterrupted.

Keywords: Internet-of-Things, Long Short-Term Memory, Reinforcement Learning, Distributed Denial of Service, Privacy Preservation, Homomorphic Encryption

1. Introduction

Internet of Things (IoT) has become a critical component of modern digital ecosystems, powering smart homes, industrial automation, healthcare monitoring, transportation systems, and large-scale sensor networks [1]. With billions of interconnected devices worldwide, IoT environments generate massive volumes of heterogeneous and continuous network traffic [2]. However, the proliferation of resource-constrained, weakly secured IoT-based smart devices has made them a prime target for cybercriminals seeking to launch various types of malicious Distributed Denial of

Service (DDoS) attack on network environments [3]. This rapid expansion have introduced severe security vulnerabilities, making IoT networks prime targets for sophisticated cyber threats, particularly Distributed Denial of Service (DDoS) attacks [4] Nevertheless, most traditional Intrusion Detection Systems (IDS) and firewalls often struggles to keep pace with these cyber threats or attacks due to high latency and delay in detection, inability to recognize low-rate or stealthy attack behaviors, lack of privacy-preserving and interpretable detection mechanism, and the static nature of the models that are commonly failing to generalize new botnets [5].

In recent years, various cybersecurity professionals have employed Artificial Intelligence (AI) and Machine Learning (ML) techniques for the development of a robust Intrusion Detection and Prevention Systems (IDPS) to effectively secure the interconnected landscape of IoT-based smart devices and the broader network ecosystem [6]. Technically, most signature-based IDS approaches often fail to detect novel or polymorphic DDoS attacks, while many machine learning-based solutions had suffer from prolonged detection times, often identifying threats only after network resources have been significantly degraded or compromised [7].

Additionally, user and device privacy had always been a major concern for most IoT-based environment. However, various researcher studies had utilized different cryptographic methods to safeguard user and device privacy. This includes the Advanced Encryption Standards (AES), Elliptic Curve Cryptograph (ECC), and Homomorphic Encryption (HE). These techniques are usually employed to protect data integrity and confidentiality, and secure multi-party computation to facilitate data sharing among IoT devices without compromising sensitive information [8].

This paper proposes a robust framework for real-time detection and prevention of IoT-based Distributed Denial of Service (DDoS) attacks in network environments. The proposed framework integrates the detection capabilities of Long Short-Term Memory (LSTM) networks, the proactive prevention strategies offered by reinforcement learning, and the advanced cryptographic method of Homomorphic Encryption (HE). By combining these cutting-edge techniques, this paper did not only aim to effectively identify and mitigate DDoS attacks but also to significantly bolster user and device data privacy. This multifaceted approach ensures a robust defense mechanism that adapts to evolving threats while maintaining the confidentiality and integrity of sensitive information transmitted across the network.

2. Related Works

Distributed Denial of Service (DDoS) attacks have emerged as one major pressing concern within IoT networks, requiring serious attention and investigation. These types of attacks often exploit limited resources, and disrupt the functionality of applications and services connected to the entire IoT ecosystem. [9] provided a comprehensive examination of the effects of DDoS attacks in IoT contexts, outlining the considerable harm they pose.

[10] propose a novel anomaly-based IDS specifically designed to address the challenges posed by Mongolian DDoS attacks. The system is equipped with advanced detection algorithms that enable it to identify unusual patterns of behavior in network traffic, facilitating the timely detection of these stealthy attacks even when the attack sizes from individual sources are minimal.

[6] presented a novel Adaptive Hybrid Case-Based Neuro-Fuzzy System (HCBNFS) for enhancing Intrusion Detection and Prevention Systems (IDPS) in IoT-based networks and environments. The proposed hybrid model integrated Case-Based Reasoning (CBR) for known traffic pattern detection and a Neuro-Fuzzy System (NFS) for investigating unknown traffic. The proposed HCBNFS achieved a 99% accuracy rate, alongside 99.5% for precision, recall, and F1-Score, underscoring its effectiveness in securing IoT smart home environments against cyber threats.

The paper of [11], addresses the growing threat of DDoS attacks within the IoT ecosystem and proposed an enhanced IDS which used an improved Long Short-Term Memory (LSTM) model based on honeypot-generated data. The model integrates Conv1D, Bidirectional LSTM, Bidirectional Gated Recurrent Unit (Bi-GRU), and dropout layers to effectively extract temporal and spatial features from IoT traffic. Further, the model was tested on the real-world IoT-DH dataset, and the system achieved an impressive accuracy of 99.41% and an AUC score of 0.9999. The paper of [12], emphasized the analysis of inner botnet traffic to enhance the detection and prevention of DDoS attacks. This innovative approach employed attention-based deep learning models to effectively analyze traffic sequences among bots within the source network, thereby enabling a proactive intervention at the attack's origin. The comparative evaluations against other traditional ML models using the BOT-IoT dataset demonstrated that the integration of the attention mechanism significantly boosts the F1-score to 99.5%, highlighting the model's superior performance in DDoS attack prevention. Furthermore, given the sensitivity of IoT device data, several studies have integrated cryptographic techniques in the development of a more robust privacy preservation mechanism. [13] investigated the use of Elliptic Curve Cryptography (ECC) as a robust cryptographic technique to enhance node-level security and privacy in IoT environments. Nonetheless, by harnessing the strengths of Identity-Based Encryption (IBE) and ECC, which allows for strong security with smaller key sizes, their paper assessed the performance and security implications of ECC for securing data transmission at the IoT network edge. [14] leveraged the Federated Learning techniques to create a global behavioral fingerprinting model for a target object by analyzing its interactions with various peers in the network. Their approach enabled distributed training of the model while incorporating a secure delegation strategy that involves less capable IoT nodes. Additionally, the integration of homomorphic encryption and blockchain technology ensures the privacy of both the target object and participating nodes, enhancing the robustness of the system against potential attacks.

3. Methodology and System Design

This paper utilized features from the Canadian Institute for Cybersecurity Intrusion Detection (CICIDS2017) benchmark dataset for testing and evaluation of the proposed system. The selected features for anomaly detections are the timestamp, flow duration, flow bytes, total fwd packets, and average packet size for the LSTM detection module because they capture temporal and traffic-behavior patterns relevant to DDoS attack detection. Additionally, for the privacy-preservation mechanism, the system utilized features such as IP addresses (source and destination), port numbers, and payload-related information. The selected sensitive identifiers or features is treated as sensitive attribute and encrypted using Homomorphic Encryption (HE).

The system was designed using an Object-Oriented Design Approach (OODA) while the structural component design was achieved using Unified Modelling Language (UML). The high-level architectural design of the proposed system is captured in Figure 1.

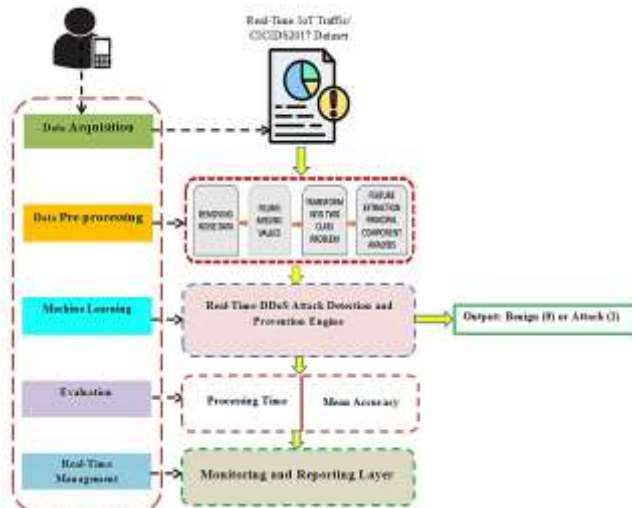


Figure 1: Architectural Design of the Proposed System

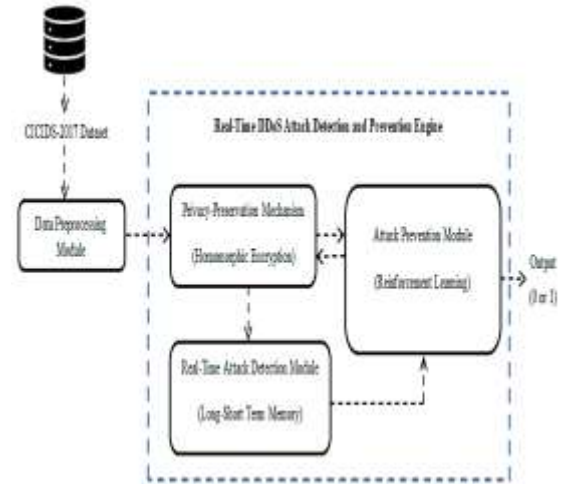


Figure 2: Component Design of the Proposed System

It captures how the network traffic data is acquired from the application layer and fed into the proposed system. Embedded in the proposed Real-Time DDoS Detection and Prevention System is a real-time attack detection engine which is designed using the techniques of LSTM to detect potential DDoS attack patterns using network traffic data. Furthermore, there is an automated response or DDoS attack prevention mechanism which is carefully designed by utilizing the techniques of Reinforcement Learning. This module is responsible for mitigating attacks when they occur. Lastly, for robust privacy-preservation, the work employs the cryptography method and design of Homomorphic Encryption (HE). This enhances the system's ability to protect data both in-transit and at-rest. Presented in Figure 2 is the component design of the proposed system. The first component is the Data Acquisition Module. This module is responsible for collecting real-time network traffic or importing the collected benchmark CICIDS2017 dataset for offline training and evaluation. It captures the flow-based traffic records, including source and destination information, protocol type, packet statistics, and time-based attributes. The module ensures that network traffic is structured into flow-level records suitable for analysis.

Further, the collected traffic data is fed into the privacy-preservation module. This module is responsible for keeping sensitive user or device data safe. It employs Homomorphic Encryption cryptographic method to encrypt all sensitive data both in-transit and at-rest. Furthermore, the collected traffic data is preprocessed and fed into the proposed attack detection module which will then determine if the traffic is benign or malicious using the techniques of LSTM. If the incoming network traffic data is malicious, the attack detection module will then forward the malicious network traffic data to the attack prevention module. This module utilizes the robust technique of reinforcement learning to further investigate the incoming traffic, classify it and take decision or action. The output of the system is in the form of zero (0) or one (1) which signifies benign or malicious traffic respectively. This work utilized the UML 2.0 sequence diagram to describe the dynamic interaction between the proposed system components during real-time DDoS detection and mitigation. It is used for illustrating how objects will communicate in a time-ordered manner from traffic capture to mitigation execution. Figure 4 captures the sequence diagram of the proposed system.

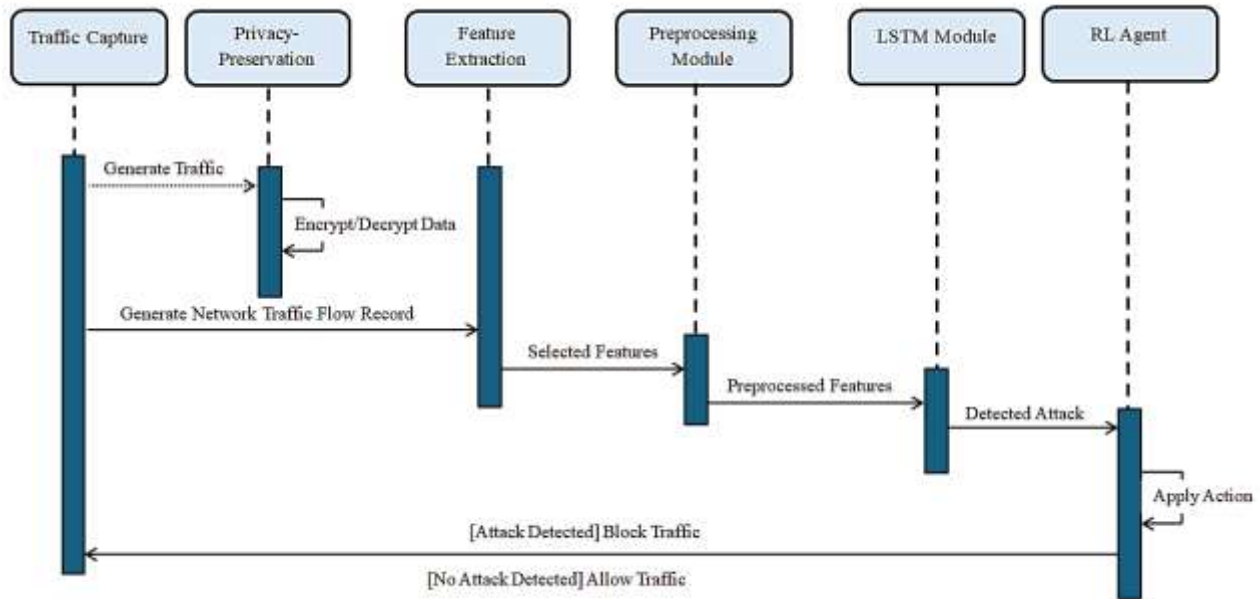


Figure 4: Sequence Diagram of the Proposed System

The process begins when the user or IoT-based network environment generates incoming traffic. The TrafficCapture object captures packets and aggregates them into flow records. These flow records are then passed to the FeatureExtraction object for statistical feature computation. Further, the extracted or selected features are transmitted to the Preprocessing object, where normalization and sequence windowing are performed. If privacy preservation is enabled, the features are passed to the PrivacyPreservation object for encryption using the CKKS scheme before further processing. The processed feature sequence is then forwarded to the LSTMDetectionEngine. The LSTM performs forward propagation using its internal gates (input, forget, output gates) and computes the probability of attack occurrence. If the predicted probability exceeds the predefined threshold, the traffic will be classified as malicious. Furthermore, upon detection of malicious traffic, the module will send a detection signal to the RLPreventionAgent. The agent will observe the current state, which includes detection confidence and network performance metrics obtained from the LSTM Detection Module. Here, the selected mitigation action is forwarded to the mitigation controller for execution. The sequence will iterate continuously as new traffic arrives, allowing the system to learn optimal mitigation strategies over time. Additionally, this will demonstrate how the proposed system integrates detection, prevention, monitoring, and privacy preservation in a continuous and adaptive feedback loop suitable for real-time IoT-based DDoS attack environments.. This work utilizes activity diagram to capture and model the behavioral flow of control between the various system component and modules. Presented in Figure 5 is the activity diagram of the proposed system.

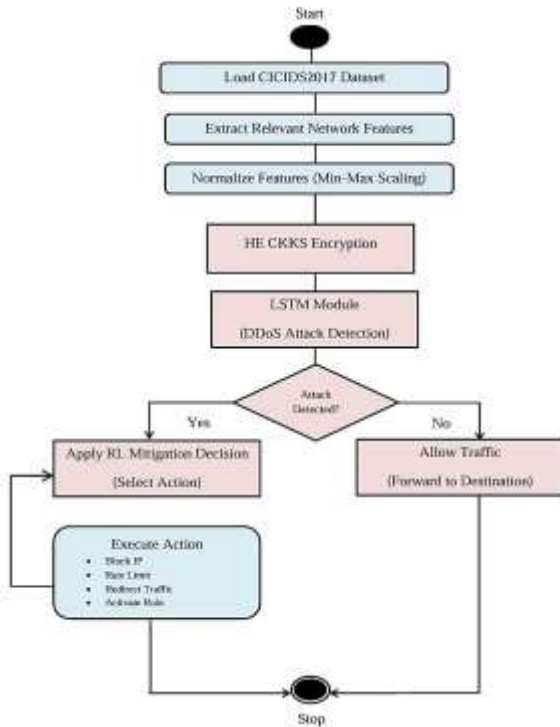


Figure 5: Activity Diagram of the System

The activity diagram illustrates the operational process of the proposed system for real-time detection and prevention of IoT-based Distributed Denial of Service (DDoS) attacks. The process begins with the loading of the dataset, which serves as the source of network traffic data for the system. After loading the dataset, the system extracts relevant network features required for analysis. These features include parameters such as packet size, protocol type, source and destination IP addresses, and traffic flow characteristics. The extracted features are then normalized using Min-Max scaling to ensure that all values fall within a uniform range, thereby improving the efficiency and accuracy of the machine learning model. Following preprocessing, the normalized data is secured using Homomorphic Encryption (HE) based on the CKKS scheme. For this paper, this step ensures that sensitive data can be processed without exposing it in its raw form, thereby preserving privacy within the IoT network environment. The encrypted data is then passed into the Long Short-Term Memory (LSTM) module, which serves as the core detection engine of the system. The LSTM model analyzes the sequential network traffic patterns and determines whether the observed behavior corresponds to normal activity or a potential DDoS attack. If no attack is detected, the system allows the network traffic to pass through and be forwarded to its intended destination without interruption. However, if an attack is detected, the system activates the Reinforcement Learning (RL) module to determine the most appropriate mitigation strategy. The RL module selects an optimal action based on learned experiences and environmental feedback. These actions may include blocking suspicious IP addresses, applying rate limiting to control traffic flow, redirecting traffic, or activating predefined security rules. Once the appropriate action is selected, it is executed by the system to mitigate the detected attack. The process then continues, ensuring continuous monitoring and protection of the network. Finally, the system completes the cycle and returns to a stable state after handling the traffic accordingly.

The proposed system utilized MongoDB, due to its flexibility in handling unstructured and semi-structured data typical of IoT environments. The database is used to store the selected network traffic data, homomorphic encrypted keys, sensitive data, incident logs, alert history etc. The logical design of the proposed system's database is presented in Figure 6

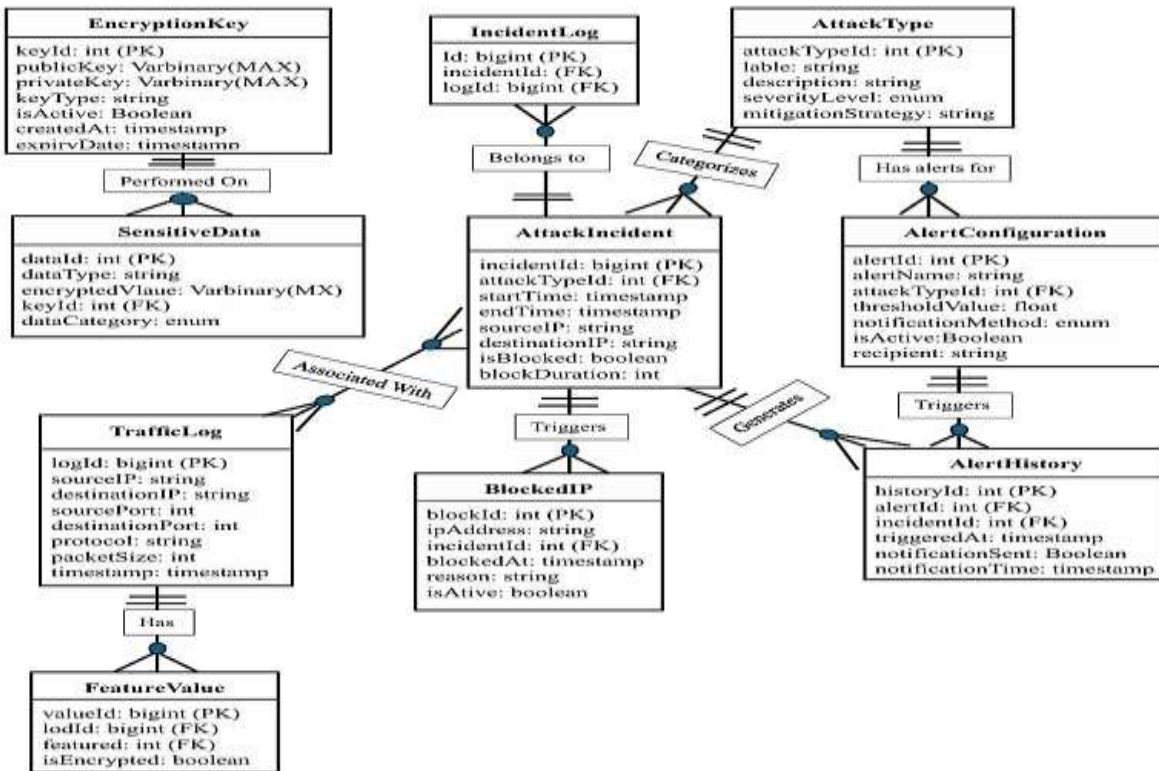


Figure 6: Logical Design of the Proposed System Database

4. Implementation and Results

The system was implemented using Python programming language with MongoDB as its database server. Further, the system was trained and testing using the collected CICIDS2017 sample IoT-based DDoS dataset on a 70%-30% split ratio. The Real-Time attack detection module was designed using the techniques of LSTM to identify low-rate and stealthy IoT-Based DDoS attack patterns. Five (5) features were selected as input variables to this module. The selected feature parameters include the Timestamp, flow duration, flow bytes, total fwd packets, and the average packet size. Figures 7, 8 and 9 capture the system's screenshot interface showing the real-time traffic scan, the output of the test conducted for Benign Traffic and DDoS attack respectively.

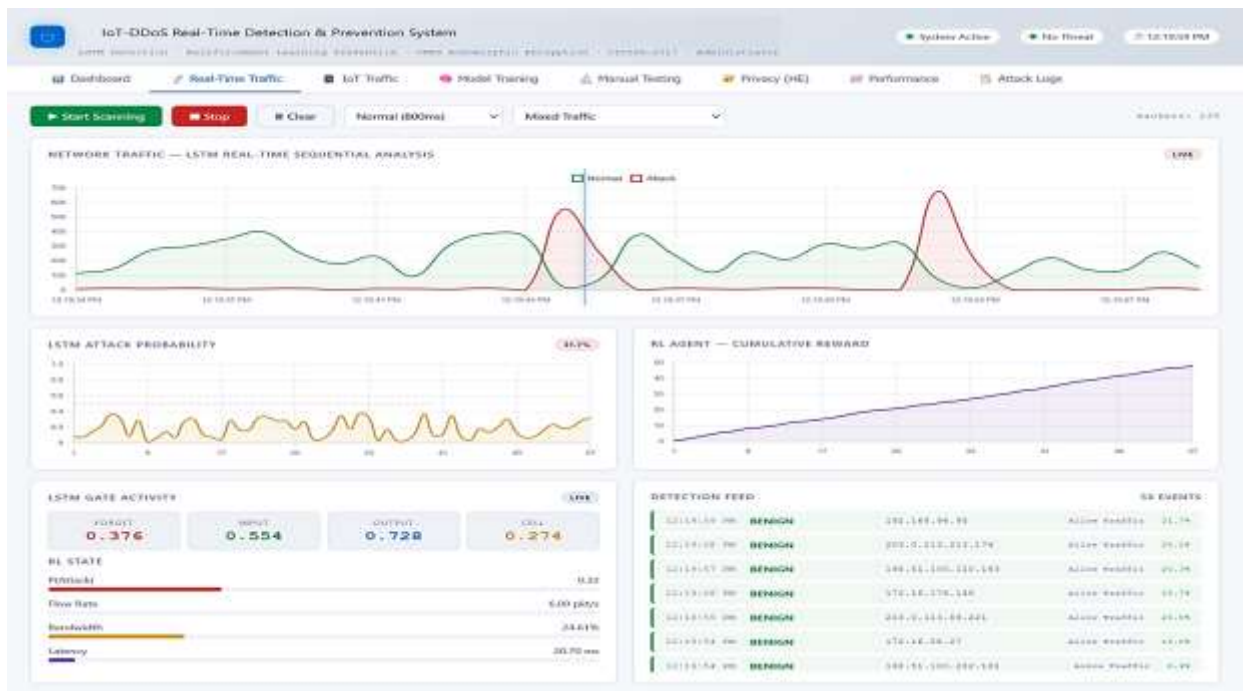


Figure 7: System Screenshot Interface for Real-Time Traffic Scanning

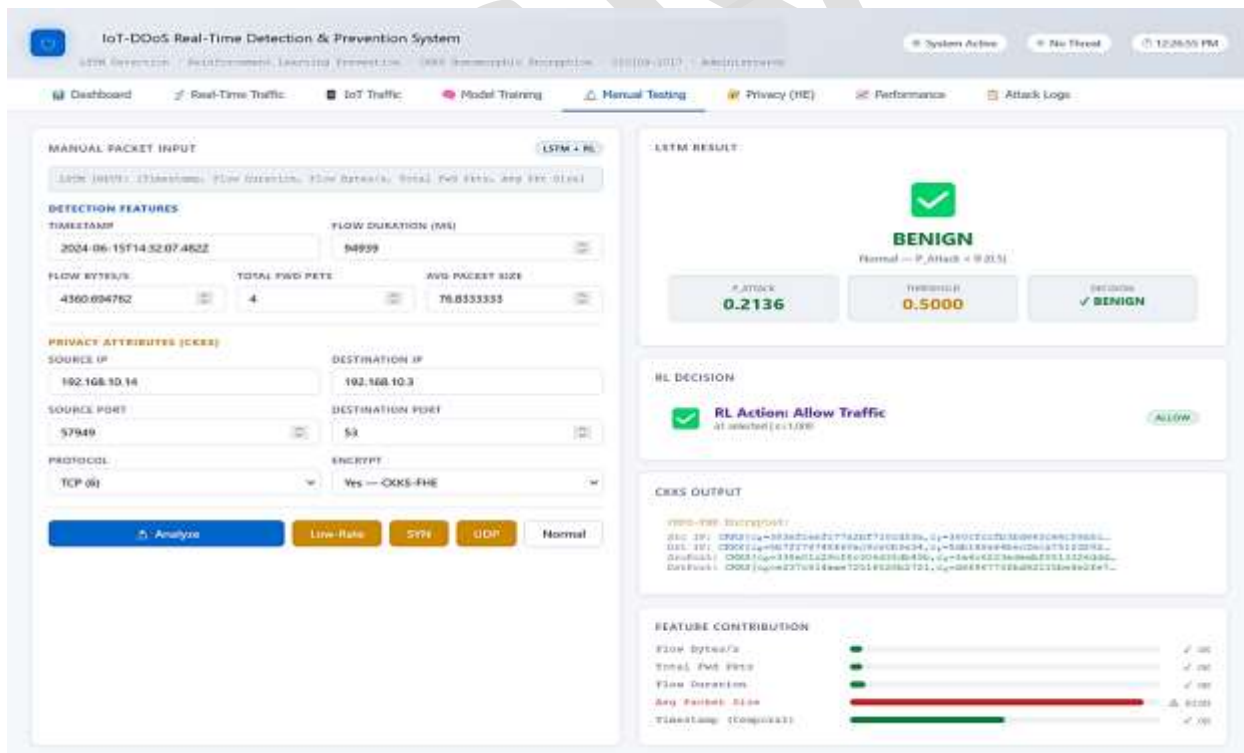


Figure 8: System Screenshot Interface for Tested Parameter for Benign Traffic

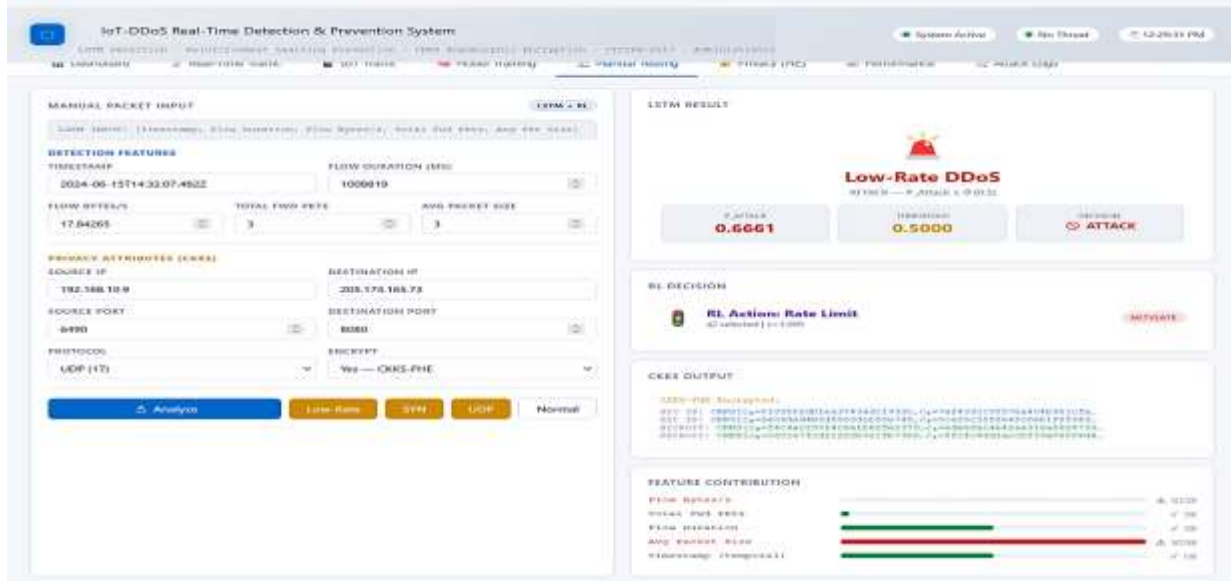


Figure 9: System Screenshot Interface for Tested Parameter for DDoS Attack

5. Conclusion

This paper presented a real-time intelligent framework for the detection and prevention of DDoS attacks in IoT-based network environments. The proposed framework integrated a Long Short-Term Memory (LSTM) deep learning model for accurate real-time attack detection, a Reinforcement Learning (RL) technique for adaptive attack prevention and mitigation, and Homomorphic Encryption (HE) using the Cheon-Kim-Kim-Song (CKKS) scheme to preserve the privacy of sensitive network traffic during storage, transmission, and processing. By combining these techniques, the developed system addressed the major limitations of conventional intrusion detection and prevention systems, including delayed detection, poor adaptability to evolving attack patterns, static response mechanisms, and inadequate privacy protection. The system was implemented using Python programming language with MongoDB serving as its database server. The paper utilized the CICIDS2017 dataset for training and evaluation of the developed system. Experimental results demonstrated that the proposed system achieved an excellent detection and prevention performance, recording a detection accuracy of 98.3%, precision of 97.8%, recall of 98.6%, and F1-score of 98.2%. Similarly, the reinforcement learning prevention module achieved an attack-blocking accuracy of 99.2% with a low false positive rate of 0.8%, confirming its effectiveness in dynamically mitigating malicious traffic while allowing legitimate network communications to proceed uninterrupted. Furthermore, the implemented CKKS homomorphic encryption mechanism successfully protected sensitive network attributes without compromising the correctness of data processing, thereby providing an additional layer of security and privacy within the proposed framework. The findings of this paper demonstrated that integrating deep learning, reinforcement learning, and privacy-preserving cryptographic techniques provide a robust and efficient cybersecurity solution for modern IoT-based network environments. The system does not only enhances the accuracy and responsiveness of DDoS attack detection and mitigation but also strengthens data confidentiality during security analysis. Consequently, this paper contributes a practical and scalable approach toward improving the resilience, reliability, and security of IoT-enabled network infrastructures against increasingly sophisticated DDoS attacks.

References

- [1] A. A. K. Majhi and S. Mohanty, "A comprehensive review on internet of things applications in power systems," *IEEE Internet of Things Journal*, 2024.
- [2] G. Mathur, R. K. Singh, M. Rakhra, and D. Prashar, "Optimizing quality control in IIoT-based manufacturing: Leveraging big data analytics and IoT devices for enhanced decision-making strategies," in *Quality Assessment and Security in Industrial Internet of Things*, ed: CRC Press, 2024, pp. 32-46.
- [3] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the Internet of Things (IoT): A survey," *Sensors*, vol. 22, p. 1094, 2022.
- [4] M. H. Ali, M. M. Jaber, S. K. Abd, A. Rehman, M. J. Awan, R. Damaševičius, *et al.*, "Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT)," *Electronics*, vol. 11, p. 494, 2022.
- [5] A. Fausto, G. Gaggero, F. Patrone, and M. Marchese, "Reduction of the delays within an intrusion detection system (ids) based on software defined networking (sdn)," *IEEE Access*, vol. 10, pp. 109850-109862, 2022.
- [6] I. N. Davies, O. E. Taylor, V. I. E. Anireh, and E. O. Bennett, "Adaptive Hybrid Case-Based Neuro-Fuzzy Model for Intrusion Detection and Prevention for Smart Home Network," *International Journal of Computer Sciences and Engineering*, vol. 10, pp. 01-10, 2024.
- [7] S. Ahmadi, "Evolving botnet defenses: A survey of machine learning approaches for identifying polymorphic and evasive malware," *International Journal of Innovative Research and Scientific Studies*, vol. 8, pp. 338-347, 2025.
- [8] N. Mohammad, "Enhancing security and privacy in multi-cloud environments: A comprehensive study on encryption techniques and access control mechanisms," *International Journal of Computer Engineering and Technology (IJCET)*, vol. 12, pp. 51-63, 2021.
- [9] A. Pakmehr, A. Aßmuth, N. Taheri, and A. Ghaffari, "DDoS attack detection techniques in IoT networks: a survey," *Cluster Computing*, vol. 27, pp. 14637-14668, 2024.
- [10] K. Doshi, Y. Yilmaz, and S. Uludag, "Timely detection and mitigation of stealthy DDoS attacks via IoT networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, pp. 2164-2176, 2021.
- [11] A. K. B. Arnob, M. Mridha, M. Safran, M. Amiruzzaman, and M. R. Islam, "An Enhanced LSTM Approach for Detecting IoT-Based DDoS Attacks Using Honeypot Data," *International Journal of Computational Intelligence Systems*, vol. 18, pp. 1-22, 2025.
- [12] S. Malekzadeh, S. Yousefi, and M. S. Tajbakhsh, "DDos prevention in IoT networks by analyzing source-side inter-bot traffic using deep learning techniques," *The Journal of Supercomputing*, vol. 81, p. 742, 2025.
- [13] I. N. Davies, O. E. Taylor, A. V. Ike, and B. E. Okoni, "Node-Level Privacy Preservation Mechanism in Internet-of-Things Network using Elliptic Curve Cryptography," *Journal of Applied Computer Science & Mathematics*, vol. 18, pp. 29-36, 2024.
- [14] M. Arazzi, S. Nicolazzo, and A. Nocera, "A fully privacy-preserving solution for anomaly detection in iot using federated learning and homomorphic encryption," *Information Systems Frontiers*, vol. 27, pp. 367-390, 2025.