Journal of Information Systems Engineering and Management
2025, 10(28s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing IoT Network Security with Deep Learning-Based Anomaly Detection

Vinay Tila Patil [1], Shailesh Shivaji Deore [2], Hemant Narottam Chaudhari [3]

[1] Research Scholar, SSVPS's Bapusaheb Shivajirao Deore College of Engineering, Dhule, Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon, Maharashtra, India. Email: vinayt.patil@outlook.com

[2] Research Guide and Associate Professor, Department of Computer Engineering, SSVPS's Bapusaheb Shivajirao Deore College of Engineering, Dhule, Maharashtra, India. Email: shaileshdeorel@gmail.com

[3] Research Scholar, Mahakaushal University, Jabalpur, Madhya Pradesh, India. Email: hemantch09@gmail.com

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has introduced unprecedented vulnerabilities, with Distributed Denial of Service (DDoS) attacks posing a major threat to the stability and security of IoT networks. This study provides a comprehensive comparison of deep learning models for detecting DDoS attacks in IoT environments. Six models—Gated Recurrent Units (GRU), Convolutional Neural Networks (CNN), Long Short-Term Memory Networks (LSTM), Deep Neural Networks (DNN), Support Vector Machines (SVM), and Logistic Regression (LR)—were evaluated on the CICDDoS2019 dataset. Each model's performance was assessed across metrics including accuracy, precision, recall, F1-score, and their ability to detect both normal and attack traffic. DNN demonstrated superior overall performance, achieving the highest accuracy (99.89%) and attack detection rate. GRU emerged as a balanced option for detecting both normal and attack traffic, while CNN excelled in attack-specific detection. The study also highlights lightweight mitigation strategies and analyses the models' throughput, offering insights into their scalability for real-time deployment. These findings provide a foundation for improving DDoS detection systems, ensuring the robustness and security of IoT networks against evolving threats.

Keywords: IoT Security, Distributed Denial of Service (DDoS), Anomaly Detection, Gated Recurrent Unit (GRU), Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), Deep Neural Network (DNN), CICDDoS2019 Dataset.

INTRODUCTION

The amount of data traversing the Internet is rapidly increasing due to the growing popularity and complexity of connected devices and software solutions. End-user usage of network resources is rising, driven by social networks, web banking applications, e-commerce platforms, and more. As a result, new cloud-based services have become essential for operating this increasingly dynamic network environment, necessitating specific requirements such as dynamic traffic allocation [1][2][55]. Moreover, the exponential growth of Internet of Things (IoT) devices is transforming the Internet landscape, increasing the heterogeneity of communication due to the unique network requirements and processing capabilities of each device [3][4]. These changes make traditional static network environments impractical for ensuring effective management and security [5][6].

In the context of IoT networks, Distributed Denial of Service (DDoS) attacks pose a significant threat due to the interconnected and heterogeneous nature of IoT ecosystems. DDoS attacks exploit network vulnerabilities to disrupt operations, making efficient detection and mitigation strategies vital for securing IoT environments [49]. Among emerging approaches, Software-defined Networking (SDN) offers a promising paradigm for IoT network management and security [7][8]. SDN centralizes network management into a programmable controller, which can communicate with and control devices such as routers and switches, irrespective of their manufacturer, creating a flexible and scalable infrastructure. By decoupling the control and data planes, SDN enables dynamic, programmable, and on-demand network configurations, offering a foundation for next-generation IoT networks [9].

However, the centralization of SDN introduces a critical vulnerability: the SDN controller becomes a potential target for attackers. Malicious actors may target the controller using techniques like intrusions [10][11] or DDoS attacks [12][13][14]. Thus, robust protection mechanisms are required to maintain network availability and ensure the quality of IoT services [16].

DDoS attacks and other intrusions can be generically described as anomalies, which occur when network behaviour deviates from its normal state [17][50]. Although anomaly detection has been widely studied, the field remains open for research due to the diversity of network scenarios and architectures [18][15]. The unique characteristics of IoT networks, such as heterogeneous devices, resource constraints, and dynamic traffic patterns, make DDoS detection particularly challenging.

Among anomaly detection approaches, IP flow-based methods have demonstrated efficiency in various environments, including IoT networks. These methods analyse network flows to characterize normal operation with high precision. However, most research in this area relies on sampling processes, analysing data in intervals ranging from several minutes to just a few seconds [19][20][21][22][23]. While sampling facilitates scalability, it risks missing stealthier attacks, such as port scans. Analysing individual flows without sampling offers a more precise detection approach, enabling the identification of anomalies in specific communications.

In this paper, we propose a defence system for IoT networks against DDoS attacks, based on single IP flow analysis. This approach allows for faster detection and mitigation of anomalies, ensuring the quality and reliability of IoT services. The system consists of two main modules: Detection and Mitigation. The Detection Module uses deep learning models, including Gated Recurrent Units (GRU), as binary classifiers to detect anomalies in individual IP flows. GRU is particularly well-suited for scenarios requiring the analysis of historical data, making it effective for anomaly detection in IoT networks [24][25][26]. The Mitigation Module generates efficient countermeasures to address detected attacks by identifying the source of the anomaly and implementing a targeted response.

To evaluate the proposed system, we utilized the publicly available **CICDDoS2019 dataset** [27], which includes a wide variety of DDoS attack types and provides comprehensive IP flow features. The dataset allows for the application of deep learning-based detection methods and enables the evaluation of mitigation efficiency. Performance metrics such as accuracy, precision, recall, and F1-score were used to compare the proposed GRU-based detection system with other shallow and deep learning models [49]. Additionally, the system's ability to process network flows per second was measured to assess its scalability and practicality in real-world IoT scenarios.

The main contributions of this paper are as follows:

- A system for detecting and mitigating DDoS attacks in IoT networks, leveraging deep learning models for anomaly detection.
- A precise detection scheme based on isolated IP flow analysis, enabling near real-time detection and rapid mitigation responses.
- A comparative evaluation of GRU and other shallow and deep learning models using the CICDDoS2019 dataset.

The remainder of this paper is organized as follows: Section 2 reviews related work; Section 3 describes the organization of the proposed system; Section 4 details the GRU method used for anomaly detection; Section 5 discusses performance outcomes, including comparisons with other detection methods and mitigation evaluation; and Section 6 concludes with future directions.

RELATED WORKS

The Internet of Things (IoT) has revolutionized the digital landscape by connecting billions of devices and enabling seamless communication across heterogeneous networks. However, this interconnectivity has also introduced significant vulnerabilities, particularly Distributed Denial of Service (DDoS) attacks, which threaten the availability and stability of IoT networks. Anomaly detection techniques, powered by machine learning (ML) and deep learning (DL) models, have emerged as effective methods for identifying and mitigating these threats. Several studies have explored machine learning techniques for network anomaly detection. For instance, Nanda et al. [28] proposed using ML algorithms trained on historical data to detect network attacks. They compared the performance of various ML algorithms, including C4.5, Bayesian Network, Decision Table, and Naive Bayes, with Bayesian Network achieving around 91% prediction accuracy. Similarly, Kornycky et al. [29] applied ML methods, such as kNN, GMM, and TRAP-VQ, to classify traffic in wireless networks, demonstrating the efficiency of ML in traffic characterization and security monitoring.

In addition to shallow ML methods, the recent emergence of deep learning (DL) techniques has revolutionized anomaly detection in network environments. DL algorithms, such as Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRU), have shown superior performance due to their ability to process sequential and temporal data. For example, Qin et al. [30] applied LSTM networks to detect anomalies in IP networks, achieving promising results in precision and recall. In [31] Kao and Jiang developed an anomaly detection framework that leveraged GRU and other statistical methods, outperforming traditional models in terms of precision, recall, and F-measure. Deep learning has also been effectively applied to IoT-specific security challenges. Guo et al. [32] demonstrated DL's potential in anomaly detection for IoT systems in smart cities, while [48] explored DL models for industrial IoT environments, emphasizing their efficiency in identifying malicious activities. Furthermore, Xie et al. [33] utilized GRU and 1D-CNN models for predicting sensor parameters in industrial control systems, achieving high accuracy and precision. Qu et al. [34] proposed a modified GRU model for identifying user anomalies in web logs, showing better performance compared to traditional LSTM and SVM approaches.

Anomaly detection often involves analysing traffic data in intervals, such as 5 minutes [19][20] or smaller intervals like 1 minute [23]. While this approach helps with scalability, it may overlook subtle, stealthy attacks like port scans. Recent studies have highlighted the importance of analysing individual traffic flows to ensure faster and more precise anomaly detection. Liu et al. [35]) proposed a GRU-based method combined with Principal Component Analysis (PCA) for dimensionality reduction and anomaly detection. Their model, validated on the KDD Cup 99 dataset, demonstrated improved efficiency compared to classical ML approaches. Building on these findings, our work focuses on leveraging deep learning models for detecting DDoS attacks in IoT networks. Unlike sampling-based methods, our approach analyses individual IP flow data to provide near real-time detection. Using GRU, we perform a multidimensional analysis of multiple flow features to classify traffic as normal or anomalous. By addressing challenges unique to IoT environments, such as heterogeneity and resource constraints, our proposed system ensures faster detection and mitigation of DDoS attacks, minimizing their impact on IoT networks.

IOT DEFENCE SYSTEM FOR DDOS DETECTION

In this section, we describe the operation of the proposed defence system for detecting and mitigating DDoS attacks in IoT networks. The interconnected and heterogeneous nature of IoT devices makes them particularly vulnerable to attacks, necessitating robust and efficient defence mechanisms. The proposed system focuses on the analysis of multidimensional IP flows to detect anomalies, including DDoS attacks, in real-time. Unlike traditional approaches that analyse traffic data over time windows (from seconds to minutes), the proposed system analyses individual flows to improve detection accuracy and response time for mitigation actions. While this approach involves processing large volumes of data, it offers the advantages of rapid detection, reducing the impact of attacks on end users, and identifying attackers by utilizing qualitative information stored in IP flow records, such as source and destination IP addresses and communication ports.

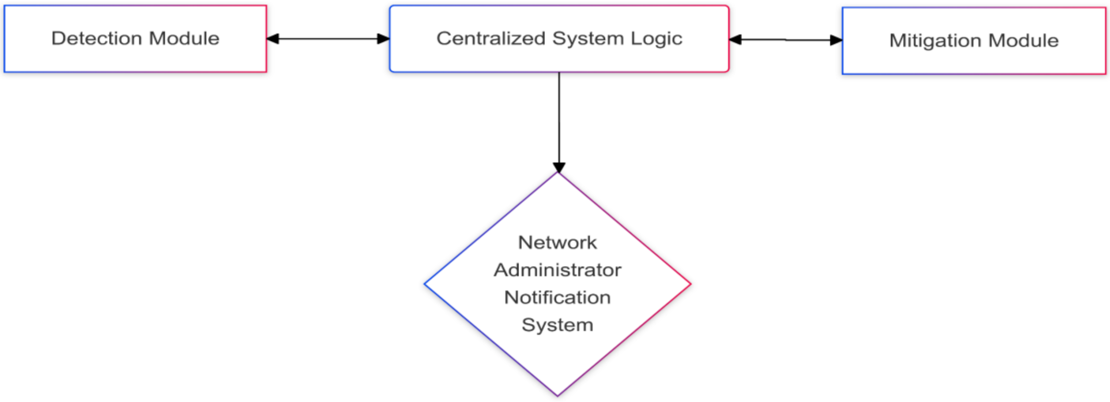

Figure 1: Modular organization of IOT defence system

The IoT defence system is composed of two main modules: the Detection Module and the Mitigation Module, which communicate through a centralized system logic, as shown in Figure 1. Each module consists of sub-modules, and the entire process operates autonomously. The network administrator receives notifications about detected attack events but is not required to intervene manually.

3.1 Detection Module

The Detection Module is responsible for identifying intrusion and DDoS attacks and triggering an alarm to invoke the Mitigation Module. In this module, a deep learning-based Gated Recurrent Unit (GRU) model is employed as the binary classifier for anomaly detection. GRU is well-suited for analysing sequential data and provides robust performance for detecting anomalies in IoT traffic.

This module consists of two sub-modules:

1. **Training Sub-Module**: Responsible for calibrating the classification model using historical labelled data.
2. **Flow Analysis Sub-Module**: Responsible for analysing IP flow records in real-time and generating binary classification results (normal or anomalous).

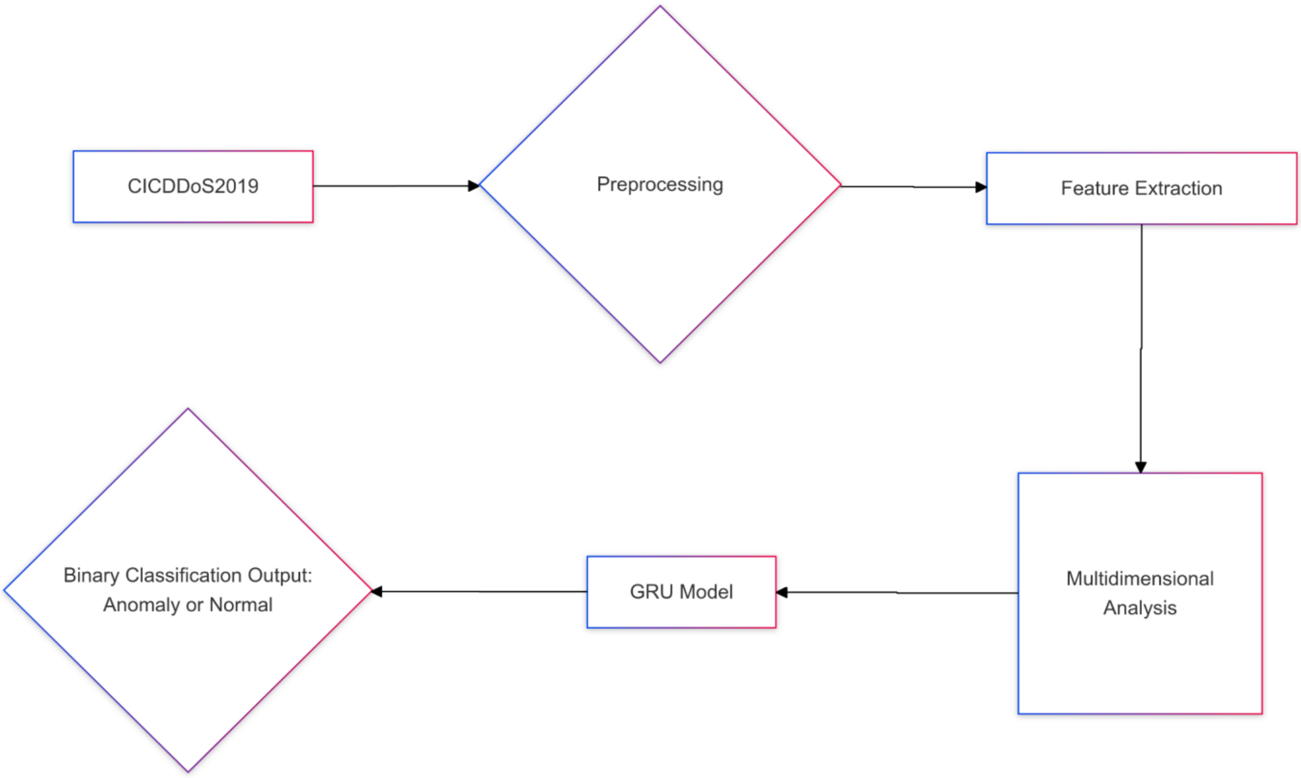
CICDDoS2019
Preprocessing
Feature Extraction
Multidimensional Analysis
GRU Model
Binary Classification Output: Anomaly or Normal

Figure 2: Detection Module

Figure 2 illustrates the flow of data within the Detection Module, highlighting how IP flow records are processed. The multidimensional analysis of IP flow features enriches anomaly detection by capturing relevant communication details, such as patterns of data transfer and participating nodes [21]. Unlike traditional methods that rely on manually selected features like packet rates, GRU automatically assigns higher importance to features that most influence classification outcomes. This capability enhances the detection of non-obvious patterns, significantly improving anomaly detection in IoT networks.

3.2 Mitigation Module

The Mitigation Module defines and implements optimal countermeasures to minimize the impact of detected attacks. It consists of two sub-modules:

1. **Countermeasure Definition Sub-Module**: Identifies the optimal mitigation action based on the detected anomaly.
2. **Drop Policy Implementation Sub-Module**: Generates and sends drop policies to the network infrastructure.

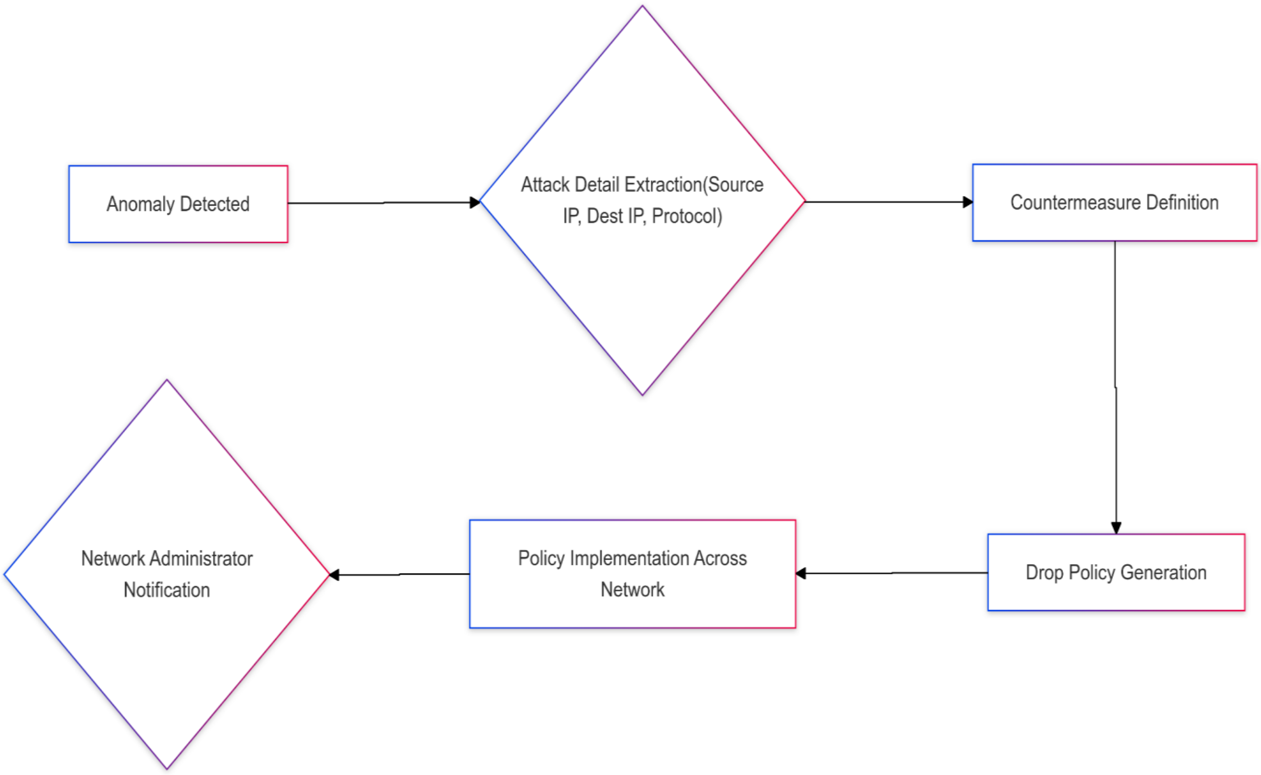
Anomaly Detected
Attack Detail Extraction(Source IP, Dest IP, Protocol)
Countermeasure Definition
Drop Policy Generation
Policy Implementation Across Network
Network Administrator Notification

Figure 3: Mitigation Module

Since the system analyses individual IP flows, it directly identifies the attacker node and discards its traffic without relying on probabilistic estimations, reducing computational overhead. Figure 3 provides an overview of the mitigation workflow, where the system extracts key information from the detected attack flow (e.g., source IP, destination IP, protocol) to generate a targeted drop policy. This policy is then implemented across the network to block malicious traffic while ensuring minimal disruption to normal operations. The directed mitigation approach enables lightweight and efficient attack responses. Upon detecting an anomaly, the system generates an alarm, invokes the Mitigation Module, and notifies the network administrator. This autonomous operation ensures fast detection and response, minimizing the impact of attacks on IoT services.

3.3 Overall System Workflow

Figure 4 presents the overall operation of the proposed IoT defence system. The process begins with the extraction of single IP flow records containing multiple quantitative and qualitative features. Qualitative features, such as the "protocol" element, are converted into numerical values using an MD5 hashing process for compatibility with the GRU model. Features like source and destination IP addresses are excluded from anomaly detection to prevent overfitting and improve generalization.

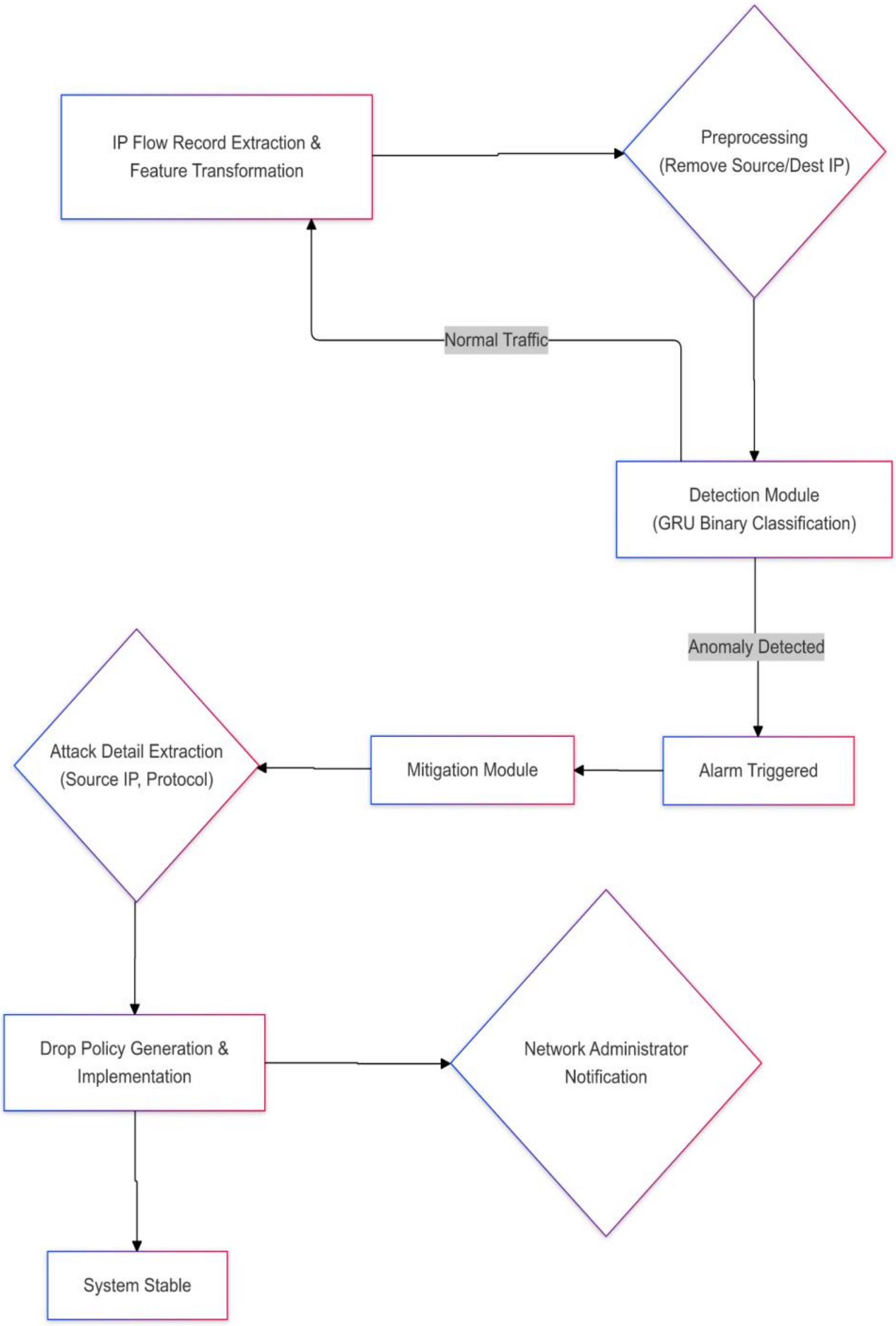
IP Flow Record Extraction & Feature Transformation
Preprocessing (Remove Source/Dest IP)
Normal Traffic
Detection Module (GRU Binary Classification)
Anomaly Detected
Alarm Triggered
Mitigation Module
Attack Detail Extraction (Source IP, Protocol)
Drop Policy Generation & Implementation
Network Administrator Notification
System Stable

Figure 4: Overall operations of IOT defence system

The processed IP flow records are submitted to the Detection Module, where the GRU-based binary classification determines if the traffic is normal or anomalous. If no anomaly is detected, the system proceeds to analyse the next flow record. If an anomaly is detected, an alarm is triggered, invoking the Mitigation Module to generate and implement the appropriate drop policy. This ensures the security and stability of IoT networks while maintaining service quality.

DEEP LEARNING METHODS FOR DDOS DETECTION

Deep learning methods are gaining increasing popularity among researchers due to their effectiveness in detecting computer network attacks and anomalies. Deep learning, a subset of machine learning, is capable of retrieving complex patterns in large datasets, making it widely applicable to tasks such as image recognition, pattern classification, and time series prediction [36] [37]. Unlike traditional "shallow" learning models, such as Multi-Layer

Perceptron (MLP), which operate with one or two layers, deep learning models utilize multiple layers of representation, enabling the discovery of complex patterns through successive layers of abstraction.

One of the significant advantages of deep learning methods is the elimination of manual feature engineering [36]. These methods automatically extract patterns from massive datasets during the training process, with weight matrices assigning importance to features that most impact classification outcomes. For IP flow protocols, which provide diverse dimensions describing network communications, deep learning models can identify subtle attack patterns that are often less evident, leading to enhanced anomaly detection accuracy.

4.1 Recurrent Neural Networks and the GRU Approach

Recurrent Neural Networks (RNNs) are particularly effective in detecting network anomalies and attacks due to their ability to handle sequential data and maintain memory of past inputs [36]. Unlike feedforward networks, such as convolutional networks, RNNs consider historical data when performing classification, which is crucial for detecting anomalies that may depend on the state of the network before the attack. RNNs iterate through sequence elements while maintaining a hidden state that retains information about previous inputs [24]. However, RNNs face the vanishing gradient problem, which limits their ability to learn long-term dependencies [38][39]. Successive operations in long-term data gradually diminish their influence, reducing their significance during the classification process. Long Short-Term Memory (LSTM) networks address this issue by implementing gated mechanisms to regulate the learning and forgetfulness rates, allowing long-term dependencies to influence predictions [40].

Gated Recurrent Units (GRUs), introduced by Cho et al. [24], are a simplified variant of LSTMs. GRUs reduce computational complexity by using fewer gates while maintaining the ability to retain long-term dependencies. While GRU and LSTM achieve similar classification accuracy [41], GRUs are faster to train due to fewer tensor operations.

In this paper, we leverage GRUs to detect DDoS and intrusion attacks in IoT environments. GRUs operate using two gates:

- **Update Gate**: Determines which information will be retained or added from the new input.
- **Reset Gate**: Controls how much of the previous information will be forgotten.

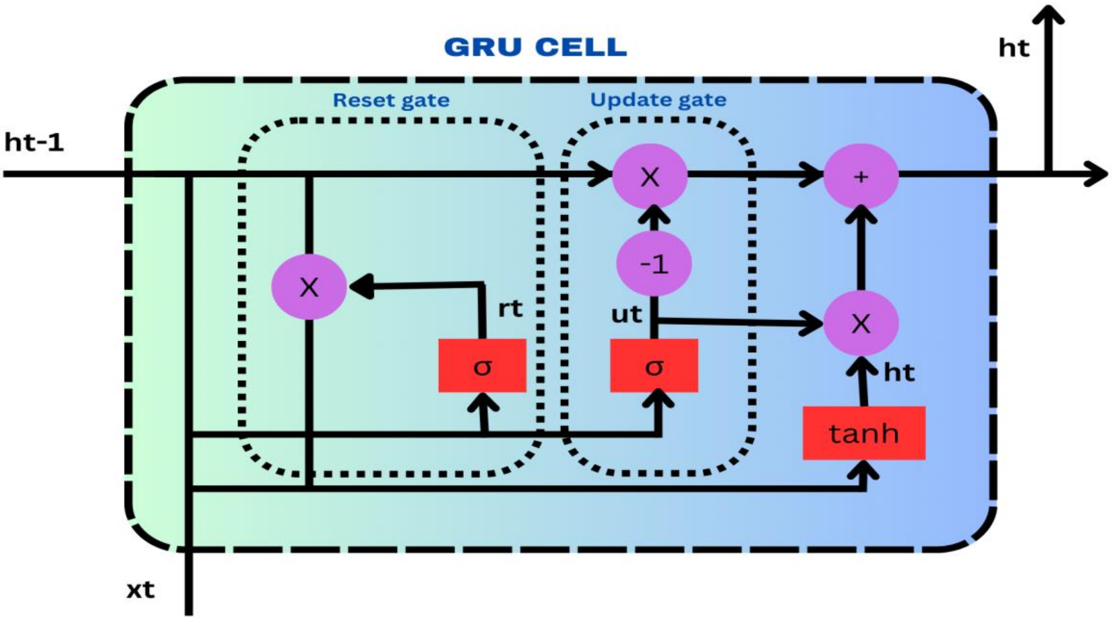

Figure 4: Representation of GRU cell

Figure 4 illustrates the internal operation of a GRU cell. The hidden state at time step ht−1h_{t-1}ht−1 and the input xtx_txt are combined and processed through these gates. The sigmoid activation function normalizes outputs to values between 0 and 1, determining which information to forget or retain. Finally, the hidden state hth_tht is updated, as described in Equation (4).

4.2 GRU Network Architecture

The architecture of the GRU network used in this study is depicted in **Figure 2**. The model consists of:

- A **GRU Layer** with 32 cells (C=32C = 32C=32).
- A **Dropout Layer** with a drop rate of 0.5 to prevent overfitting (Srivastava et al., 2014).
- A **Fully-Connected Layer** with 10 neurons (h=10h = 10h=10) for global classification.
- A **Dense Output Layer** with a sigmoid activation function for binary classification (normal or malicious traffic).

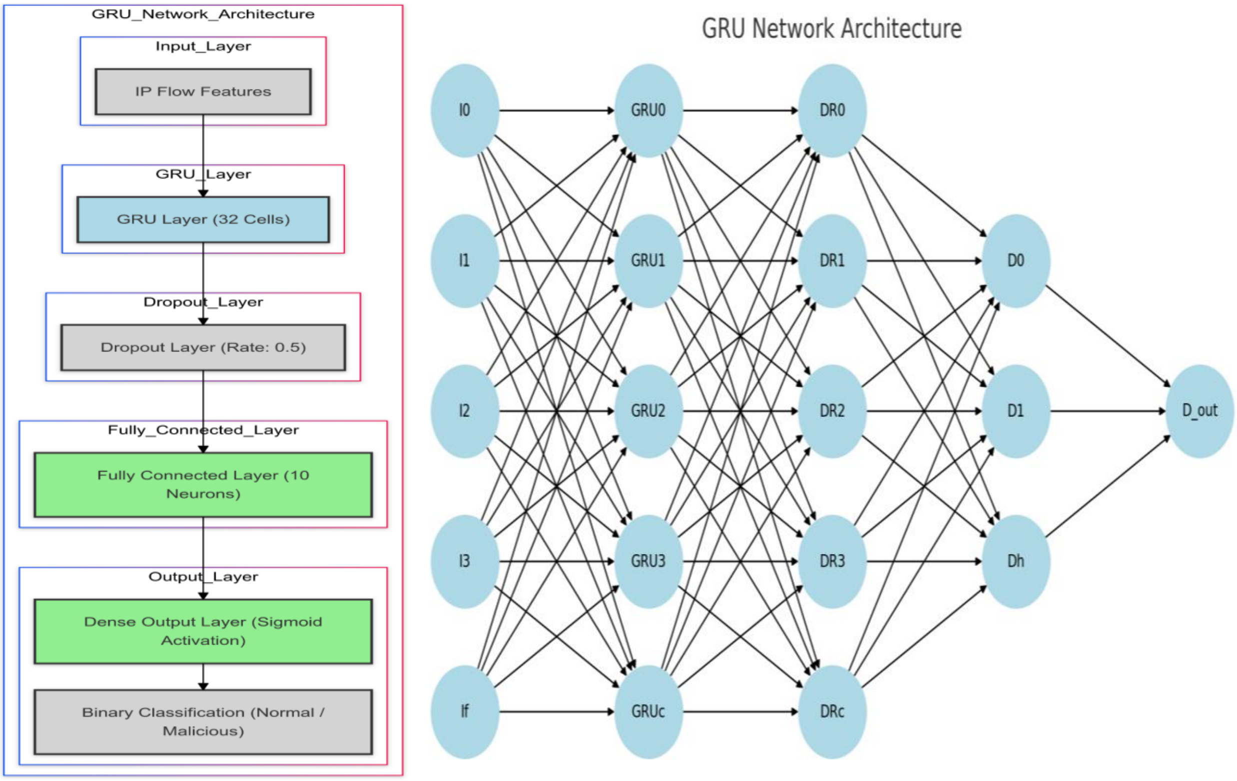

Figure 5: GRU architecture through a high-level representation(a), and through a traditional neural network representation (b)

This configuration was chosen based on extensive empirical testing using the CICDDoS2019 dataset. Figure 3 demonstrates the testing results for varying numbers of GRU cells, highlighting the trade-off between classification accuracy and flow throughput. The GRU architecture achieves an optimal balance at 32 cells, offering high accuracy while maintaining efficient processing of flows per second.

Figure 4 compares different numbers of neurons in the fully connected layer. Results indicate minimal influence of this parameter on classification accuracy beyond 10 neurons, allowing us to optimize computational costs by setting h=10h = 10h=10.

4.3 GRU Model Training and Operation

During training, the GRU model is calibrated using labelled data from the CICDDoS2019 dataset. This dataset provides a diverse range of DDoS attack patterns, enabling the GRU to generalize effectively for anomaly detection. Each IP flow is processed independently, with its features passed through the GRU layers to classify it as normal or malicious. The dropout layer mitigates overfitting by randomly ignoring neurons during training, ensuring the model remains robust. The fully connected layer aggregates features learned by the GRU cells for final classification, with the output layer providing a binary result.

This GRU-based approach offers several advantages for IoT network defence, including automatic feature extraction, efficient handling of sequential data, and reduced computational complexity compared to traditional methods.

TESTS AND RESULTS

This section evaluates the performance of the proposed GRU-based IoT DDoS detection and mitigation system. We compared the GRU approach with several other well-established detection techniques, including Deep Neural Network (DNN) [42], Convolutional Neural Network (CNN) [43][37], Long-Short Term Memory (LSTM) [30][37], Support Vector Machine (SVM) [44], Logistic Regression (LR) [45], k-Nearest Neighbors (kNN) [46], and Gradient Descent (GD) [47].

All models were implemented in Python using Keras (for GRU, LSTM, CNN, and DNN) and Sklearn (for SVM, LR, kNN, and GD). The experiments were conducted on a Windows 10 machine with an Intel Core i7 2.8 GHz processor and 8 GB of RAM. Key configurations for each model include:

- **GRU and LSTM**: Configured with 32 units.
- **DNN**: Three hidden layers with 100, 40, and 10 neurons, respectively.
- **CNN**: Three layers with 64, 32, and 16 filters and kernel sizes of 16, 8, and 3, respectively.
- **SVM**: Linear kernel.
- **kNN**: Number of neighbors set to 3.
- **LR and GD**: Default Sklearn configurations.

All methods were trained and tested for 100 epochs, as most models converge well within this range.

5.1 Evaluation Metrics

The following metrics were used to evaluate the models:

- **Accuracy**: Percentage of correctly classified IP flows.
- **Precision**: Ratio of true positives (correctly identified malicious flows) to all predicted positives.
- **Recall**: Percentage of correctly classified malicious flows (sensitivity).
- **F-Measure**: Harmonic mean of precision and recall, providing a balanced metric for classification performance.

In addition, the number of IP flows processed per second by each method was measured to evaluate scalability.

Method	Accuracy	Precision	Recall	F1_Score	Average	Normal_Detect_Rate	Atk_Detect_Rate
GRU	0.9985	0.9992	0.9991	0.9991	0.9990	0.9959	0.9991
CNN	0.9901	0.9915	0.9967	0.9941	0.9931	0.9571	0.9967
LSTM	0.9899	0.9928	0.9950	0.9939	0.9929	0.9639	0.9950
DNN	0.9989	0.9993	0.9994	0.9994	0.9993	0.9967	0.9994
SVM	0.9986	0.9991	0.9993	0.9992	0.9991	0.9954	0.9993
LR	0.9972	0.9989	0.9977	0.9983	0.9981	0.9947	0.9977
GD	0.9987	0.9991	0.9993	0.9992	0.9991	0.9957	0.9993

5.2 CICDDoS2019 Dataset

The CICDDoS2019 dataset [27] was used to evaluate the methods. This dataset includes 12 types of DDoS attacks for training and 6 types for testing. A total of 87 features were provided, but only 83 were used, excluding “source and destination IP address,” “source port,” and “Flow ID” to prevent data bias.

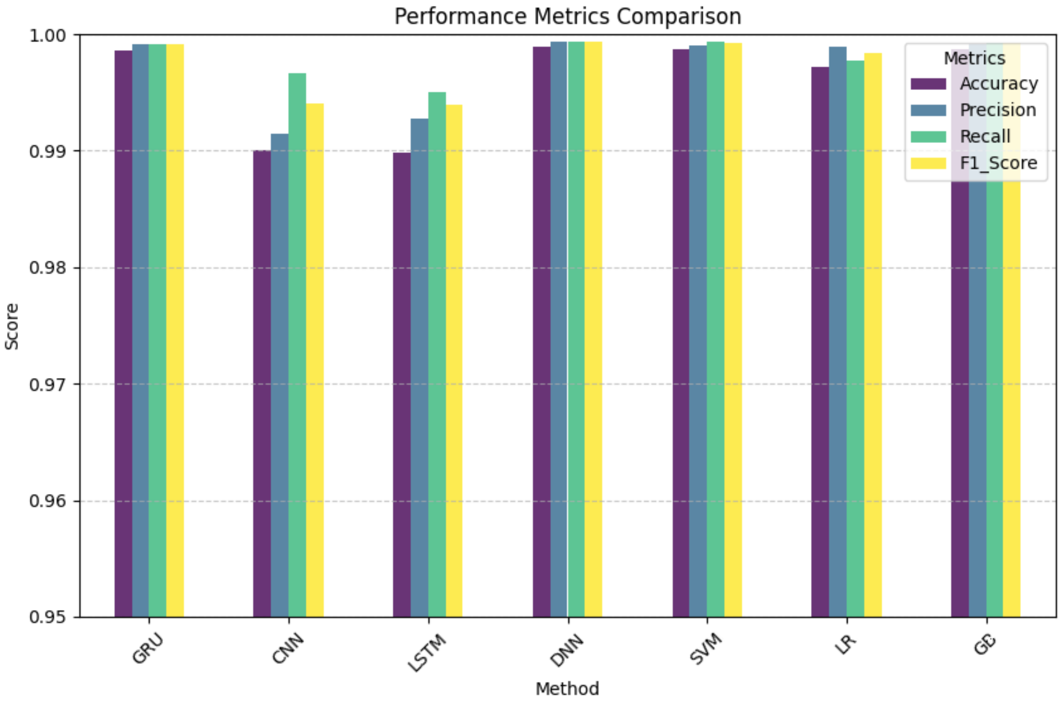

Figure 1: Performance Metrics Comparison

This bar chart presents the comparison of various machine learning models (GRU, CNN, LSTM, DNN, SVM, Logistic Regression (LR), and Gradient Boosting (GB)) based on Accuracy, Precision, Recall, and F1-Score. The GRU model demonstrates high precision and recall, making it an effective choice for anomaly detection. DNN and SVM also exhibit strong performance, whereas CNN and LSTM show slightly lower accuracy. The high precision of GRU indicates that false positives are minimal, ensuring reliable intrusion detection.

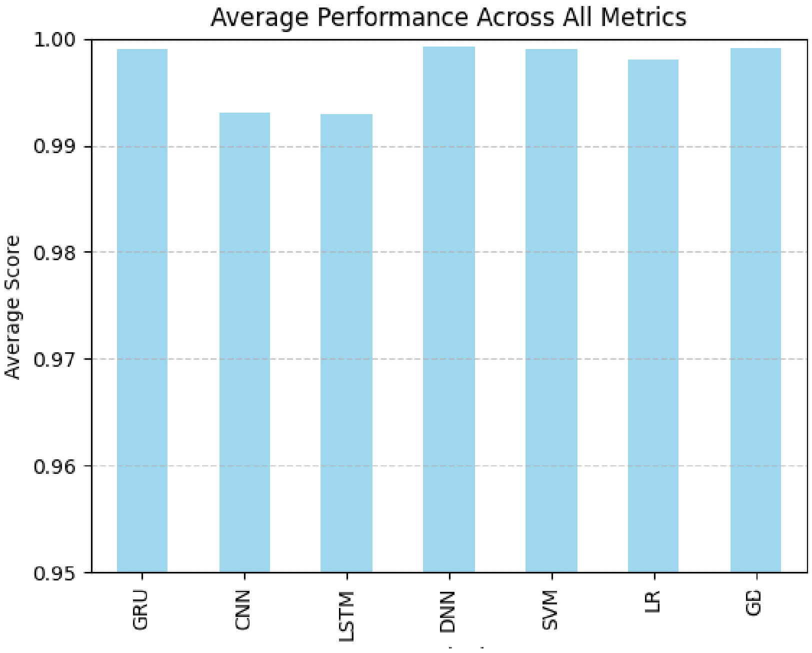

Figure 2: Average Performance Across All Metrics

This chart summarizes the overall performance of each method by computing the average score across all key metrics (Accuracy, Precision, Recall, and F1-Score). DNN, GRU, and SVM consistently achieve the highest average scores, indicating their robustness in detecting normal and attack flows. The CNN and LSTM models have relatively lower scores, suggesting they may not generalize as well for IoT network security tasks.

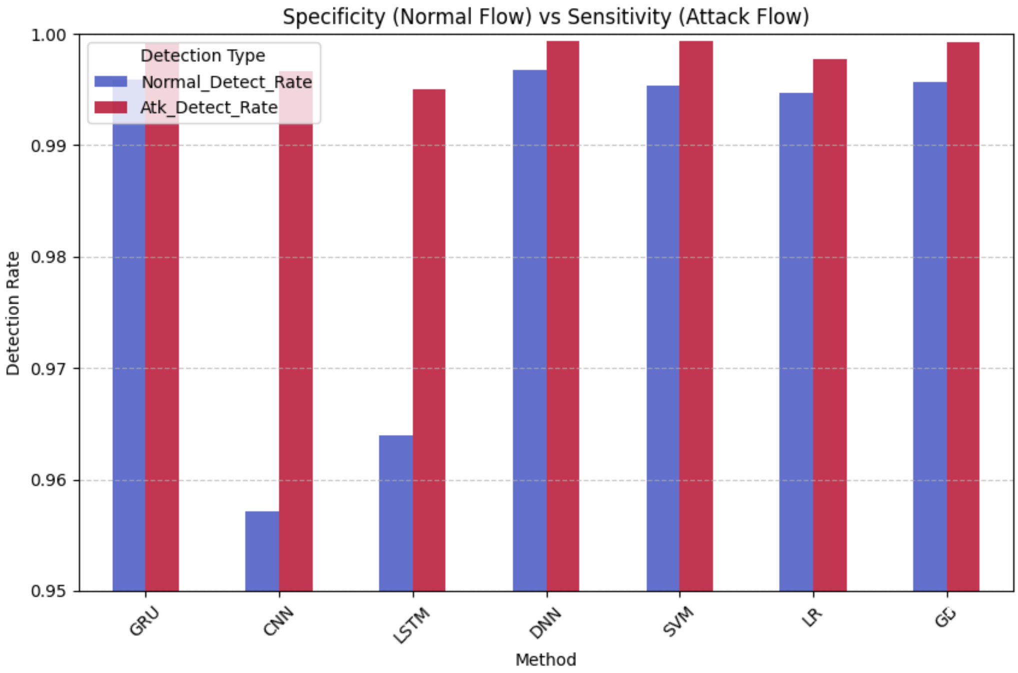

Figure 3: Specificity vs Sensitivity

This grouped bar chart illustrates the **Normal Flow Detection Rate (Specificity)** and **Attack Flow Detection Rate (Sensitivity)** for each model.

- **Specificity** (Normal Flow Detection) measures how well the model detects benign network traffic.
- **Sensitivity** (Attack Flow Detection) represents the model's ability to correctly identify malicious activity.

Observations:

- **GRU, DNN, and SVM exhibit high specificity and sensitivity**, indicating balanced detection capabilities.
- **CNN and LSTM struggle with normal traffic detection**, potentially leading to higher false positive rates.
- **DNN and SVM achieve near-perfect sensitivity**, making them effective for **real-time attack detection**.

Key Results

1. **Performance Metrics**:
   - **Figure 1**: A bar chart comparing accuracy, precision, recall, and F-measure for all methods tested on this dataset.
   - **Figure 2**: A summary chart displaying the average performance of each method across all metrics.
2. **Specificity and Sensitivity**:
   - **Figure 3**: A grouped bar chart illustrating the specificity (normal flow detection) and sensitivity (attack flow detection) for each method.

Findings:

- Most methods achieved high performance, with GRU, LSTM, SVM, and kNN performing slightly better than the rest.
- GRU exhibited the most balanced performance, achieving excellent results across all metrics.
- GRU and kNN achieved the highest specificity rates, with 99.6% and 99.7%, respectively.

CONCLUSIONS

In this paper, we proposed an IoT defence system for detecting and mitigating DDoS attacks using Gated Recurrent Units (GRU) to classify individual IP flows as normal or anomalous, leveraging the CICDDoS2019 dataset for evaluation. The system consists of a Detection Module that identifies anomalies and a Mitigation Module that applies countermeasures to minimize attack impact. GRU was chosen over Long-Short Term Memory (LSTM) for its ability to learn long-term dependencies while reducing computational complexity, making it well-suited for IoT environments. Compared against DNN, CNN, LSTM, SVM, LR, kNN, and GD, GRU consistently achieved superior accuracy, precision, recall, and F-measure. Scalability tests confirmed its efficiency in handling high-flow rates. The system also implements a directed mitigation scheme that generates individual drop policies for attacker IPs. Future enhancements include multi-label classification for identifying different DDoS attack types, optimizing the drop time window to reduce computational costs, comparing GRU with ensemble learning and Deep Reinforcement Learning methods, and deploying the system in real-time IoT environments to evaluate its performance under evolving attack patterns, further strengthening IoT network security.

REFERENCE

[1] Maenhaut, P., Moens, H., Volckaert, B., Ongenae, V., Turck, F.D., 2017. Resource allocation in the cloud: from simulation to experimental validation. In: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), pp. 701–704. https://doi.org/10.1109/CLOUD.2017.96.

[2] Patil, V. T., & Deore, S. S. (2024). DDoS attack detection: Strategies, techniques, and future directions. Journal of Electrical Systems, 20(9s), 2030–2046. https://doi.org/10.52783/jes.4808

[3] Yoon, S., Kim, J., 2017. Remote security management server for iot devices. In: 2017 International Conference on Information and Communication Technology Convergence. ICTC, pp. 1162–1164. https://doi.org/10.1109/ICTC.2017.8190885.

[4] Bera, S., Misra, S., Roy, S.K., Obaidat, M.S., 2018. Soft-wsn: software-defined wsn management system for iot applications. IEEE Systems Journal 12, 2074–2081. https://doi.org/10.1109/JSYST.2016.2615761.

[5] da Costa, K.A., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque, V.H.C., 2019. Internet of things: a survey on machine learning-based intrusion detection approaches. Comput. Network. 151, 147–157. https://doi.org/10.1016/j.comnet.2019.01.023.

[6] Hajiheidari, S., Wakil, K., Badri, M., Navimipour, N.J., 2019. Intrusion detection systems in the internet of things: a comprehensive investigation. Comput. Network. 160, 165–191. https://doi.org/10.1016/j.comnet.2019.05.014.

[7] Zehra, U., Shah, M.A., 2017. A survey on resource allocation in software defined networks (sdn). In: 2017 23rd International Conference on Automation and Computing. ICAC, pp. 1–6. https://doi.org/10.23919/IConAC.2017.8082092.

[8] Farris, I., Taleb, T., Khettab, Y., Song, J., 2019. A survey on emerging sdn and nfv security mechanisms for iot systems. IEEE Communications Surveys Tutorials 21, 812–837. https://doi.org/10.1109/COMST.2018.2862350.

[9] Zhang, S., Wang, Y., Zhou, W., 2019. Towards secure 5g networks: a survey. Comput. Network. 162, 106871. https://doi.org/10.1016/j.comnet.2019.106871.

[10] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., Lloret, J., 2017. Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot. Sensors 17. https://doi.org/10.3390/s17091967.

[11] Patil, V. T., & Deore, S. S. (2024). IoT-Guardian: Advanced detection of DDoS attacks in IoT systems using CNNs. Journal of Electrical Systems, 20(10s), 3855–3864. DOI: https://doi.org/10.52783/jes.5943

[12] Daneshgadeh Çakmakçı, S., Kemmerich, T., Ahmed, T., Baykal, N., 2020. Online ddos attack detection using mahalanobis distance and kernel-based learning algorithm. J. Netw. Comput. Appl. 168, 102756. https://doi.org/10.1016/j.jnca.2020.102756.

[13] Wang, P., Yang, L.T., Nie, X., Ren, Z., Li, J., Kuang, L., 2020. Data-driven software defined network attack detection: state-of-the-art and perspectives. Inf. Sci. 513, 65–83. https://doi.org/10.1016/j.ins.2019.08.047.

[14] Xu, J., Wang, L., Xu, Z., 2020. An enhanced saturation attack and its mitigation mechanism in software-defined networking. Comput. Network. 169, 107092. https://doi.org/10.1016/j.comnet.2019.107092.

[15] Patil, Vinay & Deore, Shailesh. (2023). A STUDY OF DDOS ATTACK DETECTION METHODS. Shu Ju Cai Ji Yu Chu Li/Journal of Data Acquisition and Processing. 38, pp. 3583-3591. DOI: 10.5281/zenodo.98549840.

[16] Correa Chica, J.C., Imbachi, J.C., Botero Vega, J.F., 2020. Security in sdn: a comprehensive survey. J. Netw. Comput. Appl. 159, 102595. https://doi.org/10.1016/j.jnca.2020.102595.

[17] Proença, M.L., Zarpelao, B.B., Mendes, L.S., 2005. Anomaly detection for network servers using digital signature of network segment. In: Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop. AICT/SAPIR/ ELETE'05, pp. 290–295. https://doi.org/10.1109/AICT.2005.26.

[18] Fernandes Jr., G., Rodrigues, J.J., Carvalho, L.F., Al-Muhtadi, J.F., Proença Jr., M.L., 2019. A comprehensive survey on network anomaly detection. Telecommun. Syst.70, 447–489. https://doi.org/10.1007/s11235-018-0475-8.

[19] Cortez, P., Rio, M., Rocha, M., Sousa, P., 2006. Internet traffic forecasting using neural networks. In: The 2006 IEEE International Joint Conference on Neural Network Proceedings, pp. 2635–2642. https://doi.org/10. 1109/IJCNN.2006.247142.

[20] Berezinski, ´ P., Jasiul, B., Szpyrka, M., 2015. An entropy-based network anomaly detection method. Entropy 17, 2367–2408. https://doi.org/10.3390/e17042367.

[21] Shuying, Chang, Qiu, Xuesong, Gao, Zhipeng, Qi, Feng, Liu, Ke, 2010. A flow-based anomaly detection method using entropy and multiple traffic features. In: 2010 3rd IEEE International Conference on Broadband Network and Multimedia Technology. IC-BNMT, pp. 223–227. https://doi.org/10.1109/ICBNMT.2010.5705084.

[22] Pena, E.H.M., Barbon, S., Rodrigues, J.J.P.C., Proença, M.L., 2014. Anomaly detection using digital signature of network segment with adaptive arima model and paraconsistent logic. In: 2014 IEEE Symposium on Computers and Communications. ISCC, pp. 1–6. https://doi.org/10.1109/ISCC.2014.6912503.

[23] Sun, D., Fu, M., Zhu, L., Li, G., Lu, Q., 2016. Non-intrusive anomaly detection with streaming performance metrics and logs for devops in public clouds: a case study in aws. IEEE Transactions on Emerging Topics in Computing 4, 278–289. https://doi.org/10.1109/TETC.2016.2520883.

[24] Cho, K., van Merri ¨enboer, B., Gulcehre, C., Bahdanau, D., Bougares, F., Schwenk, Bengio, Y., 2014. Learning phrase representations using RNN encoder–decoder for statistical machine translation. In: Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP). Association for Computational Linguistics, Doha, Qatar, pp. 1724–1734. https://doi.org/10.3115/v1/D14-1179.

[25] Lopez-Martin, M., Carro, B., Lloret, J., Egea, S., Sanchez-Esguevillas, A., 2018. Deep learning model for multimedia quality of experience prediction based on network flow packets. IEEE Commun. Mag. 56, 110–117. https://doi.org/10.1109/MCOM.2018.1701156.

[26] Aldweesh, A., Derhab, A., Emam, A.Z., 2020. Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues. Knowl. Base Syst. 189, 105124. https://doi.org/10.1016/j. knosys.2019.105124. http://www.sciencedirect.com/science/article/pii/S0950705119304897.

[27] Sharafaldin, I., Lashkari, A.H., Hakak, S., Ghorbani, A.A., 2019. Developing realistic distributed denial of service (ddos) attack dataset and taxonomy. In: 2019 International Carnahan Conference on Security Technology. ICCST, pp. 1–8. https://doi.org/10.1109/CCST.2019.8888419.

[28] Nanda, S., Zafari, F., DeCusatis, C., Wedaa, E., Yang, B., 2016. Predicting network attack patterns in sdn using machine learning approach. In: 2016 IEEE Conference on Network Function Virtualization and Software Defined Networks. NFV-SDN, pp. 167–172. https://doi.org/10.1109/NFV-SDN.2016.7919493.

[29] Kornycky, J., Abdul-Hameed, O., Kondoz, A., Barber, B.C., 2017. Radio frequency traffic classification over wlan. IEEE/ACM Trans. Netw. 25, 56–68. https://doi.org/10.1109/TNET.2016.2562259.

[30] Qin, G., Chen, Y., Lin, Y., 2018. Anomaly detection using lstm in ip networks. In: 2018 Sixth International Conference on Advanced Cloud and Big Data. CBD, pp. 334–337. https://doi.org/10.1109/CBD.2018.00066.

[31] Kao, J., Jiang, J., 2019. Anomaly detection for univariate time series with statistics and deep learning. In: 2019 IEEE Eurasia Conference on IOT, Communication and Engineering. ECICE, pp. 404–407. https://doi.org/ 10.1109/ECICE47484.2019.8942727.

[32] Guo, Y., Ji, T., Wang, Q., Yu, L., Min, G., Li, P., 2020. Unsupervised anomaly detection in iot systems for smart cities. IEEE Transactions on Network Science and Engineering 1. https://doi.org/10.1109/TNSE.2020.3027543.

[33] Xie, X., Wang, B., Wan, T., Tang, W., 2020. Multivariate abnormal detection for industrial control systems using 1d cnn and gru. IEEE Access 8, 88348–88359. https://doi.org/10.1109/ACCESS.2020.2993335.

[34] Qu, Z., Su, L., Wang, X., Zheng, S., Song, X., Song, X., 2018. A unsupervised learning method of anomaly detection using gru. In: 2018 IEEE International Conference on Big Data and Smart Computing. BigComp, pp. 685–688. https://doi.org/10.1109/BigComp.2018.00126.

[35] Liu, S., Chen, X., Peng, X., Xiao, R., 2019. Network log anomaly detection based on gru and svdd. In:2019 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking. ISPA/BDCloud/SocialCom/SustainCom, pp. 1244–1249. https://doi.org/10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00177.

[36] McDermott, C.D., Majdani, F., Petrovski, A.V., 2018. Botnet detection in the internet of things using deep learning approaches. In: 2018 International Joint Conference on Neural Networks. IJCNN, pp. 1–8. https://doi.org/10.1109/IJCNN.2018.8489489.

[37] V. T. Patil and S. S. Deore, “Deep Learning-Driven IoT Defence: Comparative Analysis of CNN and LSTM for DDoS Detection and Mitigation,” J. Inf. Syst. Eng. Manag., vol. 10, no. 8s, pp. 08–21, 2024. Available: https://doi.org/10.52783/jisem.v10i8s.951.

[38] He, T., Droppo, J., 2016. Exploiting lstm structure in deep neural networks for speech recognition. In: 2016 IEEE International Conference on Acoustics, Speech and Signal Processing. ICASSP, pp. 5445–5449. https://doi.org/10.1109/ICASSP.2016.7472718.

[39] Bengio, Y., Simard, P., Frasconi, P., 1994. Learning long-term dependencies with gradient descent is difficult. IEEE Trans. Neural Network. 5, 157–166. https://doi.org/10.1109/72.279181.

[40] Hochreiter, S., Schmidhuber, J., 1997. Long short-term memory. Neural Comput. 9, 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735.

[41] Zhang, X., Zhang, Y., Zhang, L., Wang, H., Tang, J., 2018. Ballistocardiogram based person identification and authentication using recurrent neural networks. In: 2018 11th International Congress on Image and Signal Processing. BioMedical Engineering and Informatics (CISP-BMEI), pp. 1–5. https://doi.org/10.1109/CISP-BMEI.2018.8633102.

[42] Abdulhammed, R., Faezipour, M., Abuzneid, A., AbuMallouh, A., 2019. Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. IEEE Sensors Letters 3, 1–4. https://doi.org/10.1109/LSENS.2018.2879990.

[43] Kwon, D., Natarajan, K., Suh, S.C., Kim, H., Kim, J., 2018. An empirical study on network anomaly detection using convolutional neural networks. In: 2018 IEEE 38th International Conference on Distributed Computing Systems. ICDCS, pp. 595–1598. https://doi.org/10.1109/ICDCS.2018.00178.

[44] Lei, Y., 2017. Network anomaly traffic detection algorithm based on svm. In: 2017 International Conference on Robots Intelligent System. ICRIS, pp. 217–220. https://doi.org/10.1109/ICRIS.2017.61.

[45] Yadav, S., Selvakumar, S., 2015. Detection of application layer ddos attack by modeling user behavior using logistic regression. In: 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), pp. 1–6. https://doi.org/10.1109/ICRITO.2015. 7359289.

[46] Divyatmika, Sreekesh, M., 2016. A two-tier network-based intrusion detection system architecture using machine learning approach. In: 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 42–47. https://doi.org/10.1109/ICEEOT.2016.7755404.

[47] Wijnhoven, R.G.J., de With, P.H.N., 2010. Fast training of object detection using stochastic gradient descent. In: 2010 20th International Conference on Pattern Recognition, pp. 424–427. https://doi.org/10.1109/ ICPR.2010.112.

[48] Khan, I.A., Pi, D., Yue, P., Li, B., Khan, Z.U., Hussain, Y., Nawaz, A., 2020. Efficient behaviour specification and bidirectional gated recurrent units-based intrusion detection method for industrial control systems. Electron. Lett. 56, 27–30. https://doi.org/10.1049/el.2019.3008.

[49] V. T. Patil and G. S. Chandel, “Implementation of TPA and Data Integrity in Cloud Computing using RSA Algorithm,” Int. J. Eng. Trends Technol., vol. 12, pp. 85–93, 2014. Available: 10.14445/22315381/IJETT-V12P215.

[50] Patil, Vinay Tila and Deore, Shailesh Shivaji, Strategies and Horizons in Ddos Attack Detection: An Analytical and Predictive Study. Available at SSRN: https://ssrn.com/abstract=4727005 or http://dx.doi.org/10.2139/ ssrn.4727005

[51] P. R. Patil and V. T. Patil, “Smart Forest: An IoT Based Forest Safety And Conservation System,” Int. J. Sci. Technol. Res., vol. 9, no. 3, 2020.

[52] Shailesh S. Deore, Dr. Ashok Narayan Patil (Aug. 2012), Systematic Review of Energy- Efficient Scheduling Techniques in Cloud Computing, International Journal of Computer Application, ISSN 09758887 Vol. 52, No. 15, pp. 10-14, DOI 10.5120/8275-1877, http://www.ijcaonline.org/archives/volume52/ number15.

[53] Shailesh S. Deore, Dr. Ashok Narayan Patil (October 2012), Energy- Efficient Scheduling Scheme for Virtual Machines in Cloud Computing, International Journal of Computer Application, ISSN 0975-8887 Vol. 56, No. 10, pp. 19-25, DOI 10.5120/ 8926-2999, http://www.ijcaonline.org/archives/volume56/ number10.

[54] Shailesh S. Deore, Dr. Ashok Narayan Patil (Jan. 2013), Energy- Efficient Job Scheduling and Allocation Scheme for Virtual Machines in Cloud Computing, International Journal of Applied Information System, Vol.5, No.1, pp.56-60, DOI 10.5120/ijais-450842, http://www.ijais.org/archives/volume5/number1

[55] V. T. Patil and G. S. Chandel, "Applying Public Audit-ability For Securing Cloud Data From Modification Attack," IJSRD Int. J. Sci. Res. Dev., vol. 2, no. 4, pp. 384–388, 2014.

[56] Shailesh S. Deore (March 2016), Comparison of Energy Efficient Scheduling Schemes for Private cloud Environments, International Journal of Advance Research in Computer and Communication Engineering, Vol.5 Issue3, March 2016, DOI 10.17148/IJARCCE.2016.5380, https://www.ijarcce.com/volume-5-issue3.html

[57] Shailesh S. Deore (April 2016), Joulemeter: Power Measurement for Virtual Machine in Private cloud Environments, International Advance Research Journal Science Engineering and Technology Vol.5 Issue3, March 2016, DOI 10.17148/IARJSET.2016.3414, https://iarjset.com/recent-issue-april-2016/