

The Real-Time IoT Data Security

Evelyne Hakizimana(✉) and Gennady Dik(✉)

Saint Petersburg State University, Saint Petersburg, Russia
hakkizimana@gmail.com

Abstract. Our main area of study is IoT security, including its effects and ways to mitigate them in real time. This study focuses on Distributed Denial-of-Service (DDoS) assaults, which pose a serious risk to Internet of Things networks because of the growing number of unprotected devices. We examine the characteristics of DDoS attacks, examine the strategies to detect it, especially in the African setting, and suggest a detection methodology based on algorithms from Adaptive Resonance Theory (ART) and Long Short-Term Memory (LSTM). The detection performance is evaluated using metrics such as F1-score, precision, and recall. By offering an efficient DDoS detection framework, the study helps to improve real-time IoT data security.

Keywords: Distributed Denial-of-Service (DDoS) · Real-time Detection · Long Short-Term Memory (LSTM) · Adaptive Resonance Theory (ART) · Machine Learning · Cybersecurity · Network Security · Africa

1 Introduction

The Internet of Things' (IoT) explosive growth has transformed the way devices interact, opening the door for automation and intelligent services from tech firms [1]. But this increase in connectivity has brought about serious cybersecurity issues. The most serious of these threats to IoT ecosystems are Distributed Denial-of-Service (DDoS) attacks [2], which can disrupt services and result in major operational and financial harm [3].

A DDoS assault comprises several infected devices, frequently deployed globally, flooding a target system with excessive traffic [4]. The attack's purpose is to deplete the target's resources—such as bandwidth, CPU, memory, or application capacity—thereby denying service to legitimate users [5]. In contrast to conventional DoS assaults, which come from a single source, DDoS attacks use botnets made up of thousands or millions of compromised devices, which makes detection and mitigation difficult [6].

DDoS attacks can be categorized mainly into three types: volumetric attacks, protocol attacks, and application layer attacks [7]. Volumetric attacks aim to create enormous volumes of traffic in order to overload the target's network bandwidth. DNS amplification attacks, ICMP floods, and UDP floods are a few

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025, LNCS 15898, pp. 364–374, 2026.
https://doi.org/10.1007/978-3-031-97657-5_22

examples [8]. These assaults have the ability to overload network infrastructure with traffic quantities that surpass hundreds of gigabits per second. Protocol attacks use server or firewall resources by taking advantage of flaws in network protocols. Ping of Death attacks, which transmit distorted packets to bring down systems, and SYN floods, which take advantage of the TCP three-way handshake, are frequent instances [9]. Application layer attacks the layer 7 of Open Systems Interconnection by making ostensibly valid requests to web servers or APIs, resulting in resource exhaustion, whereas protocol attacks frequently use connection status tables or CPU cycles [6]. Attacks using HTTP floods are one example. These attacks are stealthy and difficult to detect because they mimic normal user behaviour [11].

The relevance of DDoS attacks to the Internet of Things (IoT) is critical, as IoT devices often suffer from weak security configurations, default credentials, and continuous connectivity, making them prime candidates for recruitment into botnets that perpetrate these attacks [12]. These hacked devices increase the scope and severity of DDoS attacks, endangering the reliability of connected services and infrastructures as the IoT ecosystem grows quickly—it is predicted that there will be over 26.1 million devices in 2023 [13].

Understanding and preventing DDoS assaults in IoT contexts is crucial for preserving data security and service availability, especially in light of the quick growth of IoT devices and their integration into vital infrastructures [14].

2 Related Work

It is recognised that since the primary focus of this research is IoT security, more generic cybersecurity techniques might provide insightful information and possible IoT environment application [2]. For example, methods that have been thoroughly researched in traditional cybersecurity domains, such as anomaly detection and network behaviour analysis, could be modified to improve IoT security frameworks. Many strategies have been put forth and put into practice to stop and lessen DDoS attacks, especially in places like Africa where cybersecurity infrastructure may lag behind the fast growth of IoT use [3].

2.1 Hardware and Software Mitigation Tools

Businesses in South Africa are increasingly using a mix of strong firewalls, traffic scrubbing services, and DDoS mitigation devices. Together, these tools provide a layered defence strategy by detecting and filtering malicious traffic in real-time [4]. For instance, to eliminate attacks before they affect networks, SEACOM's DDoS Protect solution uses sophisticated detection algorithms and autonomous response capabilities [8]. It makes it difficult to detect attacks in real time and requires significant computing power.

2.2 Machine Learning-Based Detection

Machine learning methods have been investigated by researchers to differentiate between attack and legitimate communications [6]. Methods like K-Nearest Neighbors (KNN), Naive Bayes, and Logistic Regression have been used to identify network traffic irregularities that could be signs of DDoS attacks. These techniques use traffic characteristics such as protocol type, source IP, and packet size to categorize traffic with low false positive rates and high accuracy [10].

2.3 Cloud and Network-Level Defences

To absorb and mitigate large-scale volumetric attacks, network behavior analysis and cloud-based traffic scrubbing have been used [9]. In order to preserve service availability, these systems examine incoming packets and remove malicious ones before they enter the company network. Although SDN itself creates new vulnerabilities that need to be mitigated, its integration has also been suggested as a way to more effectively respond to attacks and dynamically manage network resources [14].

Together, these approaches highlight a trend toward combining traditional security tools with intelligent, adaptive algorithms to address the evolving nature of DDoS threats in IoT environments [4].

3 Methodology

This study proposes a hybrid detection framework leveraging Long Short-Term Memory (LSTM) and Adaptive Resonance Theory (ART) algorithms to identify DDoS attacks in IoT network traffic.

3.1 LSTM Algorithm

LSTM, a specialized recurrent neural network, is well-suited for sequential data analysis and time-series prediction because it can remember long-term dependencies. Because of this, it works well for analysing network traffic patterns over time and spotting irregularities that could be signs of DDoS attacks. By using temporal features that it has learned, LSTM is able to differentiate between malicious and legitimate traffic.

3.2 ART Algorithm

ART is a neural network model developed for stable pattern recognition and classification. It makes it possible for the system to adjust to new patterns without losing track of previously learnt knowledge. Because of its stability-plasticity balance, ART can adapt to changing attack environments where new DDoS variations are always appearing.

3.3 Detection Process

In order to reliably and real time detection of DDoS attacks in IoT environments, the detection workflow comprises a number of essential steps: The discovery process begins with the continuous collection of network traffic data from IoT devices and their associated gateways. This raw data undergoes preprocessing steps (data is validated) including noise reduction, normalization, and feature encoding to ensure compatibility with the sequential nature of the LSTM model. After preprocessing, the data is segmented into time series and passed through an LSTM network. Preliminary classification is performed by learning the temporal dependencies and patterns associated with different types of network behaviour, including both harmless and malicious activities. The output of the LSTM is a set of probability distributions over all attack categories obtained through the model's SoftMax activation function. These probability vectors are then fed into an Adaptive Resonance Theory (ART) clustering module, which groups similar results and can dynamically identify new or evolving attack patterns without retraining. The ART module increases the detection granularity by adaptively improving ambiguous or uncertain LSTM predictions, especially for unknown attack signatures. Finally, the decision module interprets the combined results of the LSTM and ART stages and determines whether the incoming network traffic represents harmless activity or one of various predefined attack types, such as DDoS, DoS, Mirai, reconnaissance, etc. This hybrid approach ensures both high detection accuracy and the ability to operate in real time, which is critical to ensuring the security of the rapidly evolving IoT ecosystem.

3.4 Evaluation Metrics

To evaluate the applied hybrid detection system, it is planned to use Evaluation Metrics, which are quantitative measures of analysis of the accuracy, performance and reliability of machine learning models.

F1-score, the harmonic mean of precision and recall, balances these two metrics to provide a comprehensive measure of the model's effectiveness, which is particularly important in imbalanced datasets common in data security. Precision measures the proportion of correctly identified attack instances among all instances classified as attacks, reflecting the system's accuracy in minimizing false positives. Recall denotes the proportion of actual attacks that were correctly detected, highlighting the system's ability to minimize false negatives.

This flowchart in Fig. 1 visualizes the sequential steps from raw IoT network data acquisition through preprocessing, model training, classification, and final evaluation to enable real-time DDoS detection.

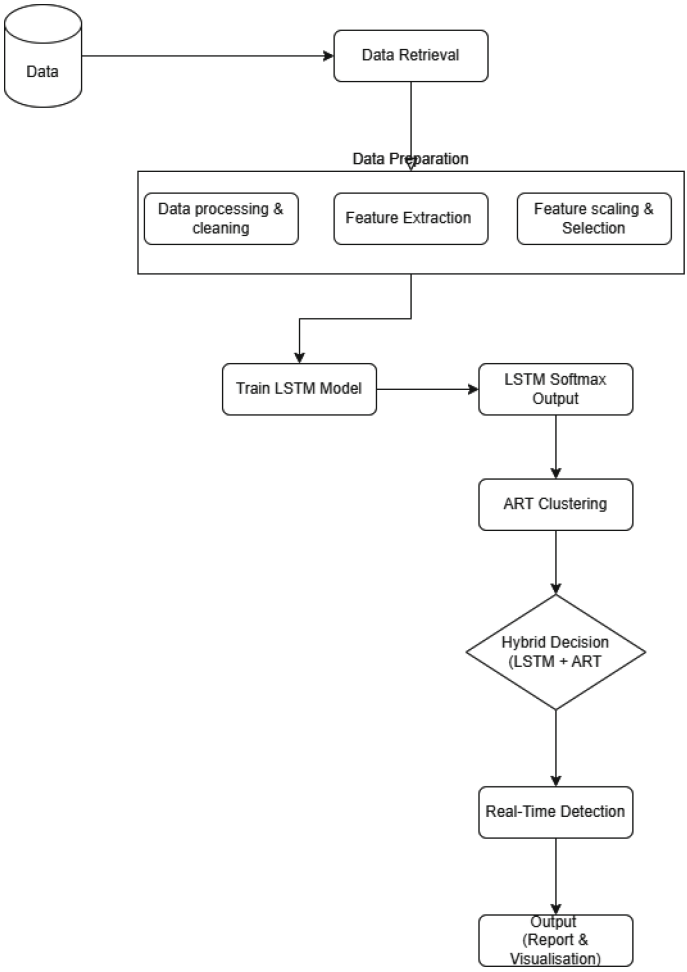

Fig. 1. Model flow chart

4 Practical Implementation

This section examines the experimental findings from our IoT network traffic dataset and presents the real-world application of the suggested hybrid LSTM-ART detection system. The assessment centres on the LSTM model's classification accuracy as well as the specific classification metrics that are obtained from F1-score, precision, and recall.

4.1 Accuracy of LSTM Model

The model's accuracy steadily increases with training, reaching a peak of over 98%. This high accuracy shows that the LSTM network is capable of learning

temporal relationships in network traffic data and differentiating between DDoS attack and normal patterns (Fig. 2).

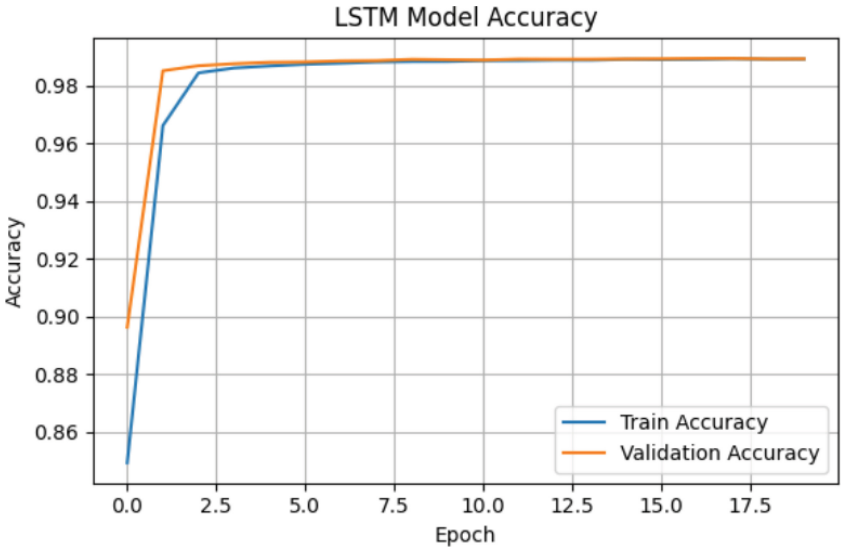

Fig. 2. LSTM model accuracy

The constant convergence of the accuracy measure demonstrates the model's ability to generalize effectively to unknown data, which is critical for real-time detection in dynamic IoT contexts. The LSTM's power to record sequential patterns enables it to detect tiny anomalies indicative of DDoS attacks (Fig. 3).

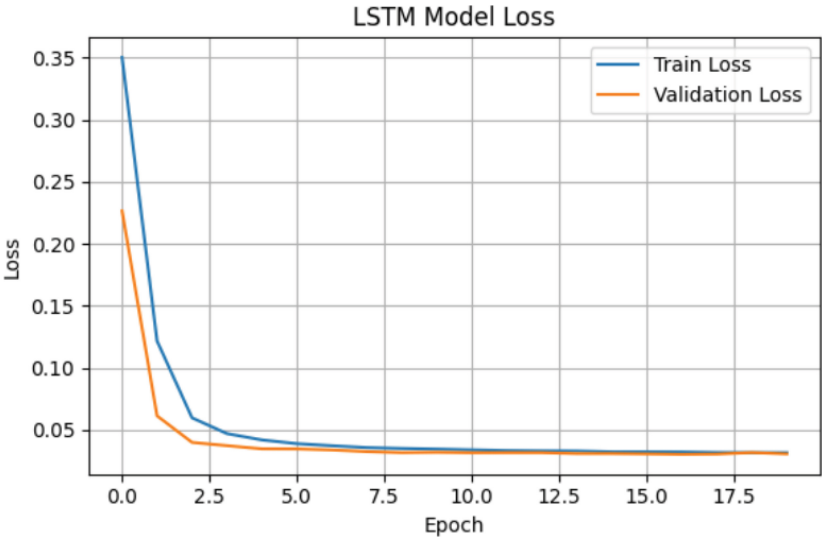

Fig. 3. Model loss convergence

4.2 Classification Report and Metrics

LSTM Classification Report:

	precision	recall	f1-score	support
Backdoor_Malware	0.00	0.00	0.00	15
BenignTraffic	0.81	0.93	0.86	4895
BrowserHijacking	0.00	0.00	0.00	28
CommandInjection	1.00	0.10	0.17	21
DDoS	1.00	1.00	1.00	152705
DNS_Spoofing	0.56	0.33	0.41	807
DictionaryBruteForce	1.00	0.11	0.19	65
DoS	1.00	1.00	1.00	36296
MITM-ArpSpoofing	0.78	0.67	0.72	1404
Mirai	1.00	1.00	1.00	11847
Recon	0.68	0.65	0.66	1427
SqlInjection	0.00	0.00	0.00	24
Uploading_Attack	0.00	0.00	0.00	5
VulnerabilityScan	0.81	0.92	0.86	162
XSS	0.00	0.00	0.00	14
accuracy			0.99	209715
macro avg	0.57	0.45	0.46	209715
weighted avg	0.99	0.99	0.99	209715

Fig. 4. Classification report and metrics

Our LSTM model provides exceptional accuracy in threat identification with flawless precision, recall, and F1 score (1.0) in DDoS categorization (Fig. 4).

4.3 Precision Recall

F1 score, and support are the metrics used in the classification report to assess the model. Recall quantifies the detection of every positive instance, whereas precision shows the accuracy of positive predictions. The F1 score is perfect for unbalanced data since it balances the two values. Support determines how many instances of each class there are in reality. When combined, these indicators offer a comprehensive picture of how well the hybrid model can identify various IoT threat types (Fig. 5).

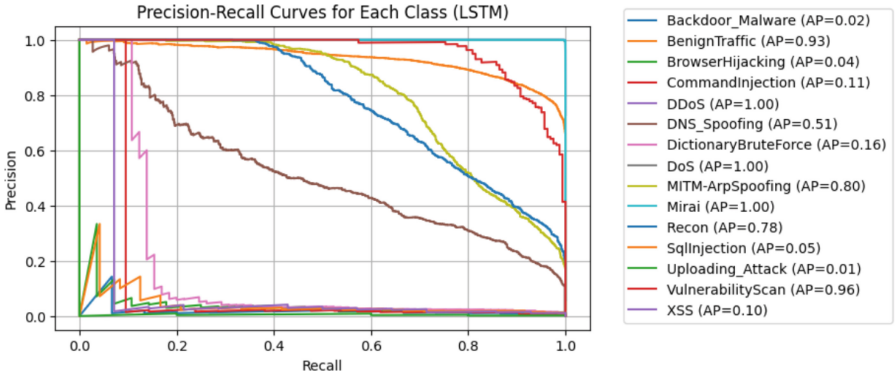

Fig. 5. Precision recall per attacks

4.4 ART Clusters on LSTM SoftMax Outputs

Adaptive Resonance Theory (ART) performs real-time clustering of the probabilistic results generated by the SoftMax layer of the LSTM. By grouping similar SoftMax distributions, ART can dynamically refine classifications and identify new or evolving attack patterns without retraining. This real-time clustering significantly improves the adaptability and responsiveness of attack detection models in rapidly changing IoT environments (Fig. 6).

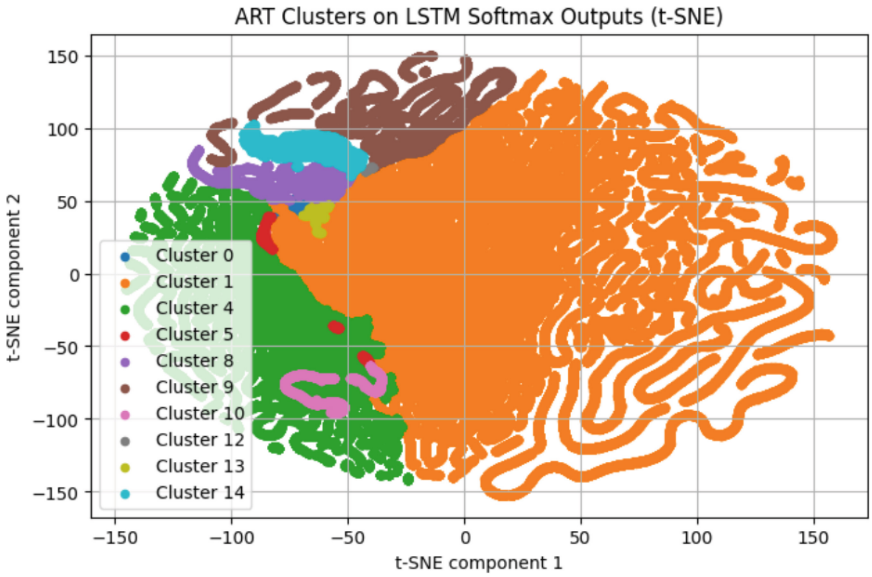

Fig. 6. ART Clustering

4.5 Number of Samples per ART Cluster

The sample distribution among ART (Adaptive Resonance Theory) clusters is depicted in this graph, which shows a notable imbalance. With more than 120,000 samples, Cluster 0 is the largest, whereas the remaining clusters (1, 4, 5, 8, 9, 10, 12, 13, 14) each have fewer than 20,000 samples. The absence of Cluster IDs (2, 3, 6, 7, 11) suggests that there was not enough similarity between the data to generate these groups. The stark difference implies that whereas smaller clusters reflect more specialized subgroups, Cluster 0 represents a dominant pattern in the data. This trend is common in ART algorithms, which frequently generate multiple specialist classifications in addition to a single major "catch-all" category. The results show ART's propensity to focus on broad patterns before identifying minor distinctions, which could be due to either intrinsic data characteristics or the algorithm's parameter sensitivity. Finding significant trends while maintaining significant outliers may be facilitated by this kind of clustering (Fig. 7).

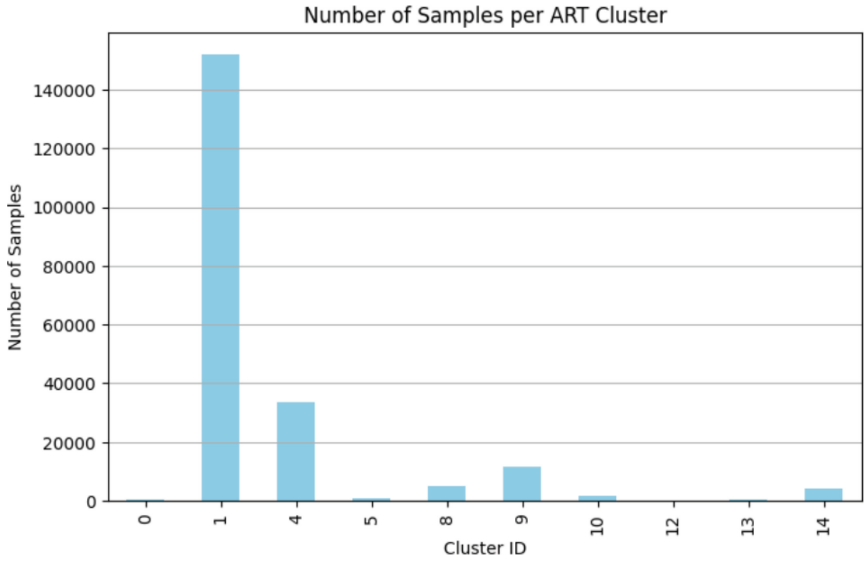

Fig. 7. Number of samples per ART Cluster

5 Conclusion

In this study, the efficacy of combining ART and LSTM algorithms for real-time DDoS attack detection in IoT environments is demonstrated. The hybrid approach uses ART's adaptive classification and LSTM's temporal pattern recognition to achieve a detection accuracy of about 98%. Evaluation using precision, recall, and F1-score metrics confirms the model's balanced performance in correctly identifying attack traffic while minimizing false alarms. These results highlight the potential of advanced machine learning techniques to improve IoT data security against increasingly complex DDoS threats, and future work may concentrate on expanding its applicability across various IoT platforms and integrating this detection system with automated mitigation strategies. Overall, by offering a strong, real-time security solution specifically designed to address the particular difficulties presented by DDoS attacks, our research helps to increase the resilience of IoT infrastructures. In conclusion, it should be noted that the practical implementation serves as an example of the possibility of combining various machine learning algorithms to ensure the security of network traffic.

References

1. Gaur, V.: Security issues in IoT-based environments. Int. Res. J. Eng. Technol. **9001**. www.irjet.net
2. Aldowah, H., Ul Rehman, S., Umar, I.: Security in internet of things: issues, challenges and solutions. In: Saeed, F., Gazem, N., Mohammed, F., Busalim, A. (eds.) IRICT 2018. AISC, vol. 843, pp. 396–405. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-99007-1_38
3. Lata, M., Kumar, V.: Challenges to IoT security: industry perspective. https://www.researchgate.net/publication/373048780
4. Ain, N.U., Sardaraz, M., Tahir, M., Abo Elsoud, M.W., Alourani, A.: Securing IoT networks against DDoS attacks: a hybrid deep learning approach. Sensors **25**(5) (2025). https://doi.org/10.3390/s25051346
5. Zhang, J., Yang, G., Lu, L., Huang, M., Che, M.: A novel visualization method for detecting DDoS network attacks (2010)
6. Bashaiwth, A., Binsalleeh, H., AsSadhan, B.: An explanation of the LSTM model used for DDoS attacks classification. Appl. Sci. (Switz.) **13**(15) (2023). https://doi.org/10.3390/app13158820
7. DDOS BACKGROUND
8. HBK-DDoS-Attack-Handbook-for-Enterprise-May-2021
9. Neto, E.C.P., Dadkhah, S., Ghorbani, A.A.: Collaborative DDoS detection in distributed multi-tenant IoT using federated learning. In: 2022 19th Annual International Conference on Privacy, Security and Trust (PST). IEEE (2022). https://doi.org/10.1109/PST55820.2022.9851984.
10. Babjan, S., Yadav, N., Mamatha, G., Sekhar, P.: A new CNN and LSTM algorithm based human activity recognition. https://doi.org/10.48047/nq.2022.20.9.nq44865
11. Sundareswaran, V.: Study of cybersecurity in data breaching. In: Int. J. Adv. Eng. Res. Dev. **5**(03) (2018). https://www.researchgate.net/publication/325300571
12. El-Sofany, H., El-Seoud, S.A., Karam, O.H., Bouallegue, B.: Using machine learning algorithms to enhance IoT system security. Sci. Rep. **14**(1) (2024). https://doi.org/10.1038/s41598-024-62861-y
13. Suvra, D.K.: An efficient real time DDoS detection model using machine learning algorithms (2025). http://arxiv.org/abs/2501.14311
14. Gnana Priya, G., Shriram, S.H., Jeeva, S., Sakthi Priya, G., Balasubadra, K.: Detection of distributed denial of service (DDoS) attack using logistic regression and K nearest neighbor algorithms. Int. J. Intell. Syst. Appl. Eng. http://www.mathtype.com