International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0237

e ISSN: 2584-2854
Volume: 03
Issue: 04 April 2025
Page No: 1460 - 1466

Enhancing Cybersecurity to Predict DDOS Attack Using Deep Learning Algorithms

A Sathiya[1], K Subashshree[2], P Abirami[3], Dr. R. G Suresh Kumar[4], Dr. S Udhayashree[5]

[1,2,3]UG Scholar, Dept of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

[4]Head of the Department, Dept of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

[5]Assitanta Professor, Dept of CSE, Rajiv Gandhi College of Engineering and Technology, Puducherry, India.

Email ID: *sathiyaa9856@gmail.com[1],srisuba2909@gmail.com[2],abiramiperumal1506@gmail.com[3], sureshkumar_rg@rgcet.edu.in[4], udhayashree_cse@rgcet.edu.in[5].*

Abstract

The increasing prevalence of Distributed Denial of Service (DDoS) attacks poses a critical threat to network security, particularly in Software-Defined Networking (SDN) environments where centralized control and programmability introduce new vulnerabilities. Traditional Machine Learning (ML) approaches for DDoS detection often struggle with outdated training data, limited adaptability to evolving threats, and high false-positive rates, limiting their effectiveness against complex traffic patterns and zero-day attacks. Recent advancements in deep learning offer promising alternatives, with hybrid models showing improved performance in dynamic environments. This survey explores the limitations of conventional ML-based detection methods and reviews recent research leveraging deep learning techniques—especially Recurrent Neural Networks (RNNs) such as Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) networks—for DDoS detection in SDN. GRU offers computational efficiency in processing sequential data, while LSTM excels at capturing long-term dependencies, making their combination a compelling choice for adaptive threat detection. This survey highlights key datasets such as CICDDoS2019, discuss current challenges, and outline future research directions, including the integration of reinforcement learning, real-time mitigation strategies, and scalable deployment for enhanced SDN security.

Keywords: *Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), hybrid algorithm, Distributed Denial of Service (DDoS).*

1. Introduction

In the evolving landscape of cybersecurity threats, Distributed Denial of Service (DDoS) attacks have emerged as one of the most disruptive and prevalent forms of cyberattacks. A DDoS attack aims to impair the normal functioning of a server, network, or website by overwhelming it with a flood of traffic originating from numerous compromised devices. Unlike a traditional Denial of Service (DoS) attack, which is launched from a single source, DDoS attacks leverage a distributed network of infected machines commonly referred to as a botnet controlled remotely by malicious actors. These devices, often unaware of their exploitation, inundate the target system with an immense volume of requests, exhausting critical resources such as bandwidth, memory, and processing power. Consequently, legitimate users face degraded performance or complete inaccessibility (Ahmad, Z. et al., 2021; Aamir, M. et al., 2021). DDoS attacks are generally classified into three main categories: volume-based attacks, which saturate bandwidth; protocol attacks, which exploit network protocol vulnerabilities; and application-layer attacks, which target specific services such as web servers or databases. Common methods include UDP floods, SYN floods, HTTP floods, and DNS amplification attacks. The increasing sophistication and scale of these attacks pose significant challenges to organizations, resulting in financial losses, operational downtime, and reputational damage (Zolanvari, M. et al., 2019; Ahmad, Z. et al., 2021).

To counter these threats, organizations employ a range of mitigation strategies, including firewalls, rate limiting, content delivery networks (CDNs), load balancers, and specialized DDoS protection services such as Cloudflare and AWS Shield. Given the growing impact of DDoS attacks on critical digital infrastructure, it is imperative to understand their mechanisms, classifications, and countermeasures [1-5]. This survey provides a comprehensive overview of DDoS attack techniques, detection methods, and defense mechanisms, highlighting current trends and future research directions in the field (Martins, N. et al., 2020; Ahmad, Z. et al., 2021).

1.1 Gated Recurrent Unit (GRU)

A Gated Recurrent Unit (GRU) is a type of recurrent neural network (RNN) designed to process sequential data while mitigating the vanishing gradient problem. It was introduced as a simpler and more efficient alternative to Long Short-Term Memory (LSTM) networks. GRUs use two gates: the reset gate, which determines how much past information to forget, and the update gate, which controls how much new information to retain. Unlike LSTM's more complex structure, GRUs combine gate functions, reducing parameters and computational load [7]. This makes GRUs faster to train and more suitable for real-time and resource-limited applications. They perform well in tasks like natural language processing, speech recognition, and time-series forecasting. While LSTM may offer finer control in some cases, GRUs provide a strong balance between efficiency and performance (Yang, Y. et al., 2020; Liu, C. et al., 2020; Su, T. et al., 2020).

1.2 Long Short-Term Memory (LSTM)

Long Short-Term Memory (LSTM) is a type of recurrent neural network (RNN) designed to handle sequential data and overcome the vanishing gradient problem. Unlike traditional RNNs, LSTM includes memory cells and three gates—input, forget, and output—that regulate information flow. The forget gate discards irrelevant data, the input gate adds new information, and the output gate determines what influences the current output. This structure enables LSTM to capture long-term dependencies, making it effective in tasks like NLP, speech recognition, and time-series forecasting. While more resource-intensive than GRUs, LSTM offers finer control over memory, making it suitable for tasks requiring deep context understanding (Su, T. et al., 2020).

2. Literature Overview

Existing approaches for DDoS detection and mitigation combine ML, SDN, blockchain, and statistical models to tackle advanced attack strategies. SDN-based frameworks with ML detect low-rate and low-density attacks effectively. Cochain-SC uses SDN and blockchain for cross-domain mitigation. Enhanced KNN models like DDADA and DDAML improve detection accuracy, while the Rhythm Matrix model distinguishes AL-DDoS attacks from flash crowds. A federated learning-based approach also emerges to enable collaborative DDoS detection across distributed networks without sharing raw data. These methods show the power of intelligent analysis and SDN in multi-layer DDoS defense.

2.1 A Flexible Sdn-Based Architecture for Identifying and Mitigating Low-Rate Ddos Attacks Using Machine Learning

This study presents a modular SDN-based framework designed to detect and mitigate Low-Rate DDoS (LR-DDoS) attacks using machine learning. The architecture integrates an intrusion detection system (IDS) trained on six ML models, achieving a 95% detection rate [6]. Implemented with the ONOS controller on Mininet, the framework simulates real-world networks and demonstrates effective attack mitigation via its intrusion prevention system (IPS). Its modular structure allows for easy upgrades and high adaptability, making it scalable for evolving SDN environments (Aamir, M. et al., 2021).

2.2 Cochain-SC: An Intra- and Inter-Domain DDoS Mitigation Scheme Based on Blockchain Using SDN and Smart Contract

This research presents Cochain-SC, a blockchain-based DDoS mitigation framework designed for both intra- and inter-domain SDN environments. It employs entropy and Bayesian methods for detecting malicious traffic within a domain, while smart contracts on the Ethereum blockchain facilitate secure and decentralized sharing of attack data across domains [8]. By combining SDN, blockchain, and smart contracts, the system effectively mitigates attacks both near their origin and along the attack path. The implementation on Ethereum's Ropsten test network validates its practicality and effectiveness in distributed DDoS defense (Yousefi, A. et al., 2020).

2.3 Hybrid DDoS Detection Framework Using Matching Pursuit Algorithm

This research introduces a hybrid DDoS detection framework leveraging the Matching Pursuit algorithm, with a focus on resource depletion and low-density DDoS attacks. It uses a dictionary generated via the K-SVD algorithm to model both normal and malicious traffic. The framework combines Matching Pursuit with artificial neural networks, achieving over 99% true positive rate and less than 0.7% false positive rate. Comparative analysis with Wavelet-based techniques confirms the superior performance of the proposed AMP method in detecting low-density DDoS attacks effectively (Karatas et al., 2020; Su et al., 2020; Jiang et al., 2020)

2.4 DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks

This research explores the use of Software Defined Networking (SDN) to defend against Distributed Denial of Service (DDoS) attacks. It proposes two detection methods: one based on the degree of DDoS attack and another using an improved K-Nearest Neighbors (KNN) algorithm enhanced with Machine Learning. Theoretical and experimental analyses demonstrate the effectiveness of these methods compared to existing solutions. Four key features and a novel concept called the "degree of attack" are introduced. The proposed algorithms, DDADA and DDAML, show superior detection performance, with plans for future implementation in real SDN environments [9-11]. Additionally, the approach enables more adaptive and intelligent network management by leveraging centralized SDN control (Liu, C et al., 2020; Ahmad, Z et al., 2021).

2.5 Identifying Application-Layer DDoS Attacks Based on Request Rhythm Matrices

This study proposes a novel statistical model called the Rhythm Matrix (RM) to detect Application-layer DDoS (AL-DDoS) attacks by analyzing user access behavior through request patterns and dwell-time values. Abnormality degrees in the RM help identify malicious hosts, with detection based on change-rate outliers. Simulation results show a True Positive Rate over 99% and a False Positive Rate under 1%. The method effectively distinguishes AL-DDoS attacks from flash crowds and demonstrates high precision and recall with optimized parameters (Nagaraja et al., 2020; Aamir et al., 2021; Ahmad et al., 2021).

3. Proposed System

The proposed system employs a hybrid deep learning model combining Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) networks for DDoS attack detection in Software-Defined Networking (SDN) environments. GRU offers computational efficiency, while LSTM effectively captures long-term dependencies in network traffic. Their integration enhances feature extraction and improves detection of complex and evolving DDoS patterns. Trained on the CICDDoS2019 dataset, the model achieves high accuracy, adaptability, and reduced false alarms. This hybrid approach enables real-time monitoring and response, ensuring network stability and security. By analyzing sequential traffic patterns, the system excels at identifying sophisticated, multi-vector attacks, thereby strengthening cybersecurity resilience in SDN networks. Additionally, the model is designed for scalability, making it suitable for deployment in large-scale and dynamic network environments without compromising performance [12].

3.1 Architectural Diagram

The architectural diagram illustrates a comprehensive workflow for DDoS attack detection using deep learning in Software-Defined Networking (SDN) environment. The process begins by loading raw network traffic data, typically in CSV format, followed by data preparation that includes cleaning, labeling, and formatting. The data is then standardized, normalized, and reduced in dimensionality to improve model performance and efficiency. After preprocessing, the dataset is split into training, validation, and testing sets for proper model development and evaluation. A hybrid ensemble model combining GRU and LSTM is trained to enhance detection accuracy and robustness. The final model enables real-time DDoS attack prediction, offering a scalable and effective solution for securing SDN environments. Figure 1 shows Architectural Workflow for ddos Detection Using Deep Learning In SDN.

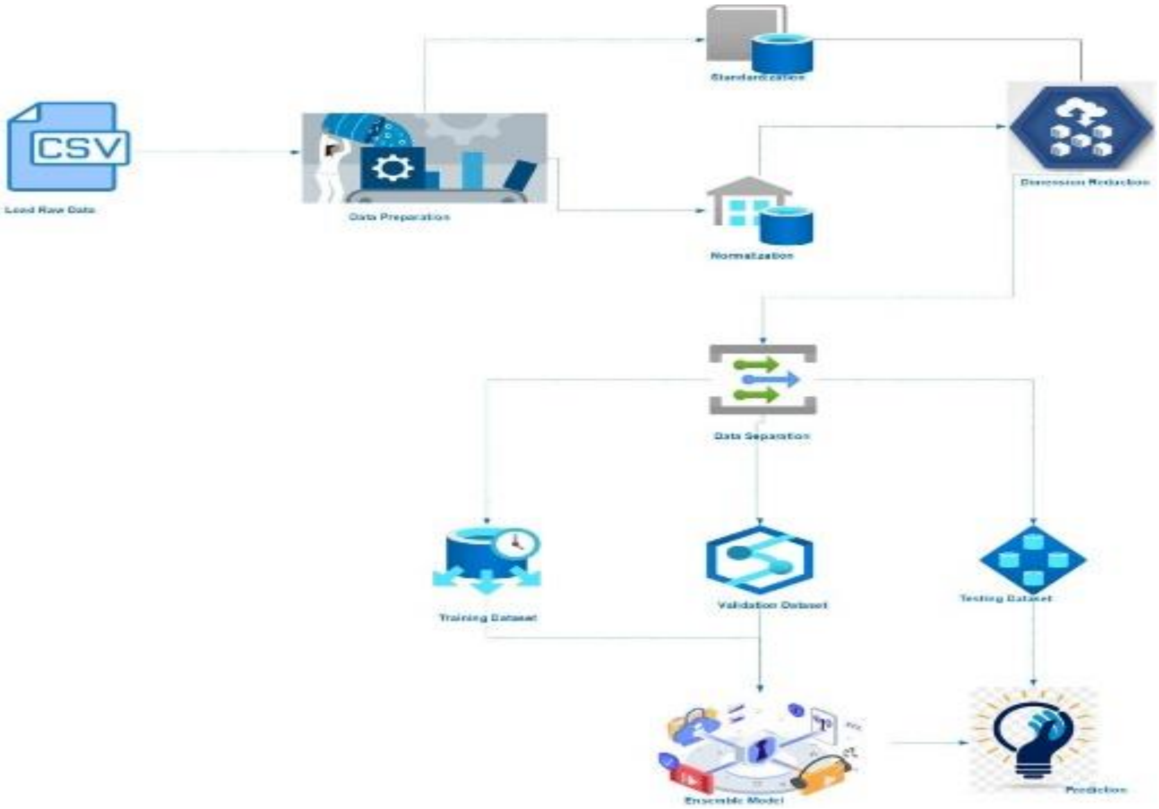

Figure 1 **Architectural Workflow for DDOS Detection Using Deep Learning in SDN**

4. Methodology and Approaches

A systematic and structured methodology was adopted to identify, review, analyze, and categorize existing literature focused on enhancing cybersecurity through the prediction and detection of Distributed Denial-of-Service (DDoS) attacks using deep learning algorithms. The approach involved collecting relevant research from reputable academic sources, applying clear selection criteria, and organizing the studies based on techniques, datasets, and evaluation metrics. Below is a detailed explanation of the methodologies adopted by key studies in the field of ddos attack detection.

4.1 Integration of Hybrid Deep Learning Architectures

To capture the complex temporal and spatial patterns inherent in network traffic data, integrating hybrid deep learning architectures proves beneficial. Combining models like Convolutional Neural Networks (CNNs) for spatial feature extraction with Long Short-Term Memory (LSTM) networks for temporal sequence learning allows for a more comprehensive analysis. CNNs excel at identifying local patterns within traffic data, such as specific byte sequences indicative of malicious payloads, while LSTMs are adept at recognizing sequential anomalies over time, such as gradual increases in traffic that may precede a DDoS event [13-15]. This synergy enables the detection system to discern both instantaneous anomalies and evolving attack patterns (Su et al., 2020; Liu et al., 2020; Yang et al., 2020).

4.2 Utilization of Real-Time Data Streams for Model Trainin

Incorporating real-time data streams into the training regimen ensures that the detection model remains adaptive to emerging threats. Traditional models trained on static datasets may become obsolete as attackers develop new strategies. By continuously updating the model with live network data, it learns to identify novel attack vectors and tactics.This approach necessitates the implementation of online learning algorithms and incremental model updates, allowing the system to evolve in tandem with the threat landscape. Moreover, real-time data integration facilitates immediate detection and response, crucial for mitigating the impact of DDoS attacks (Karatas et al., 2020; Aamir et al., 2021; Jan et al., 2019)

4.3 Scalable Implementation within Software-Defined Networking (SDN) Environment

Integrating the DDoS detection system within Software-Defined Networking (SDN) environments offers scalability and centralized control. SDN's architecture separates the control plane from the data plane, enabling dynamic and programmable network management. By deploying the detection model at the controller level, it can monitor and analyze traffic across the entire network, facilitating prompt identification and mitigation of DDoS attacks. This centralized approach allows for coordinated responses, such as rerouting traffic or implementing rate limiting, to neutralize threats effectively (Aamir et al., 2021; Jan et al., 2019; Zolanvari et al., 2019).

5. Finding and Trends: Top of Form

DDoS attacks are becoming more complex and harder to detect. Deep learning offers powerful, real-time defense by recognizing patterns and adapting to new threats. However, its success depends on high-quality, well-labeled data. The trend is moving toward combining AI with existing cybersecurity tools for smarter, faster, and more resilient protection.

5.1 Rise In ddos Attack Complexity

DDoS attacks have evolved from simple volumetric floods to sophisticated multi-vector assaults that combine protocol, volumetric, and application-layer tactics. Attackers now mimic legitimate traffic and shift techniques rapidly, making them harder to detect with static defenses. This has created a growing demand for adaptive systems capable of real-time analysis, where deep learning is proving particularly effective due to its ability to detect subtle, dynamic traffic anomalies (Yang et al., 2020; Su et al., 2020).

5.2 Deep Learning's Growing Role in Cybersecurity

Deep learning outperforms traditional methods by automatically learning complex patterns from raw data. CNNs are used for packet analysis, while RNNs and LSTMs excel at detecting time-based traffic patterns. These models improve over time through retraining, offering a scalable and intelligent defense against evolving threats, and reflecting a shift toward autonomous, AI-driven cybersecurity (Yang et al., 2020; Liu et al., 2020).

5.3 Real-Time DDoS Prediction as a Priority

Reactive defense isn't enough predictive models are now key. Deep learning enables systems to analyze live traffic, anticipate attacks, and respond in real time. This proactive approach can trigger immediate countermeasures like IP blocking or traffic rerouting, significantly reducing the damage window and enhancing overall resilience (Su et al., 2020; Yang et al., 2020).

6. Challenges and Gaps

Enhancing cybersecurity to predict DDoS attacks using deep learning involves key challenges. The high volume and complexity of attack traffic make it hard to distinguish from legitimate traffic, especially during sudden spikes. Most datasets are outdated, imbalanced, and lack diversity, leading to poor model performance and high false negatives. Deep learning models also require offline training and struggle with real-time detection, while lightweight, edge-compatible solutions for fast deployment remain underdeveloped.

6.1 High Volume and Complexity of Traffic

DDoS traffic is often obfuscated and distributed, making it difficult to distinguish from legitimate traffic. The behavior of this traffic can vary widely depending on the type of attack, such as volumetric or protocol-based, which demands highly adaptive detection models [16]. In high-speed network environments, deep learning models often struggle to process data at wire speed. Additionally, sudden bursts of traffic or flash crowds can closely resemble DDoS patterns, making accurate differentiation between real users and malicious activity more challenging (Karatas et al., 2020; Jiang et al., 2020).

6.2 Imbalanced and Non-Standardized Datasets

Most public datasets used in DDoS research, such as NSL-KDD or CIC-DDoS, fail to accurately reflect modern, real-world attack patterns. These datasets are often imbalanced, containing far more normal traffic than attack data, which causes models to overfit to benign behaviors and leads to high false-negative rates. Furthermore, the lack of diversity in these datasets hampers the cross-domain performance of trained models. Many of these datasets are outdated or synthetic in nature, limiting the models' ability to generalize and adapt to evolving attack techniques and current network architectures (D'hooge et al., 2019; Ahmad et al., 2021).

6.3 Real-time Detection Limitations

Deep learning models typically require offline training, which is time-consuming and limits the ability to quickly adapt to emerging threats. Real-time detection systems need to make fast decisions based on limited data; a requirement that clashes with the large input sizes deep models usually demand. Optimization for edge computing or lightweight deployment remains an underexplored area. Moreover, the integration of streaming data processing frameworks with deep learning for high-throughput DDoS detection is still not mature enough for practical deployment (Martins et al., 2020; Gao et al., 2019; Jan et al., 2019).

Conclusion

This survey concludes that the rise in Distributed Denial of Service (DDoS) attacks poses a severe threat to Software-Defined Networking (SDN), making traditional Machine Learning (ML) models ineffective due to their inability to adapt to evolving attack patterns. These models often struggle with outdated training data, high false-positive rates, and limited scalability, making zero-day attack detection challenging. To overcome these limitations, a hybrid deep learning approach integrating Gated Recurrent Unit (GRU) and Long Short-Term Memory (LSTM) networks is proposed. By combining GRU's efficiency in handling sequential data with LSTM's ability to capture long-term dependencies, the model enhances feature extraction and effectively detects complex attack patterns. Training the model on the CICDDoS2019 dataset ensures higher accuracy, improved adaptability, and reduced false alarms, making it more suitable for SDN environments. This hybrid approach significantly strengthens intrusion detection systems (IDS) by ensuring network stability and security. Future improvements may include reinforcement learning for adaptive attack prevention, better model scalability, and enhanced real-time mitigation mechanisms. By leveraging GRU and LSTM's strengths, the system provides a robust and computationally efficient solution to counter DDoS attacks, ensuring a resilient cybersecurity framework against evolving threats. Further research is needed to enhance the model's adaptability to emerging attack patterns, ensuring its effectiveness against evolving cybersecurity threats. Exploring the integration of advanced real-time monitoring techniques and adaptive learning mechanisms can contribute to the continuous improvement of the algorithm's responsiveness. Additionally, efforts should be directed toward scalability, enabling the algorithm to handle large-scale network environments efficiently. Collaboration with cybersecurity experts and industry practitioners can provide valuable insights for practical implementation and validation of the hybrid model in diverse network settings.

References

[1]. N. Martins, J. M. Cruz, T. Cruz, and P. H. Abreu, "Adversarial Machine Learning Applied to Intrusion and Malware Scenarios: A Systematic Review," IEEE Access, vol. 8, pp. 35403-35419, 2020. https://ieeexplore.ieee.org/document/9001114

[2]. G. Karatas, O. Demir, and O. K. Sahingoz, "Increasing the Performance of Machine Learning-Based IDSs on an Imbalanced and Up-to-Date Dataset," IEEE Access, vol. 8, pp. 32150-32162, 2020. https://ieeexplore.ieee.org/document/9018195

[3]. T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD

Dataset," IEEE Access, vol. 8, pp. 29575-29585, 2020. https://ieeexplore.ieee.org/document/8984887

[4]. H. Jiang, Z. He, G. Ye, and H. Zhang, "Network Intrusion Detection Based on PSO-XGBoost Model," IEEE Access, vol. 8, pp. 58392-58401, 2020. https://ieeexplore.ieee.org/document/9066923

[5]. A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty, and V. S. Kiran, "Similarity Based Feature Transformation for Network Anomaly Detection," IEEE Access, vol. 8, pp. 39184-39196, 2020. https://ieeexplore.ieee.org/document/9027440

[6]. L. D'hooge, T. Wauters, B. Volckaert, and F. De Turck, "Classification Hardness for Supervised Learners on 20 Years of Intrusion Detection Data," IEEE Access, vol. 7, pp. 167455-167469, 2019. https://ieeexplore.ieee.org/document/8892631

[7]. X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection," IEEE Access, vol. 7, pp. 82512-82521, 2019.https://ieeexplore.ieee.org/document/8737469

[8]. Y. Yang, K. Zheng, B. Wu, Y. Yang, and X. Wang, "Network Intrusion Detection Based on Supervised Adversarial Variational Auto-Encoder with Regularization," IEEE Access, vol. 8, pp. 42169-42184, 2020. https://ieeexplore.ieee.org/document/9042356

[9]. C. Liu, Y. Liu, Y. Yan, and J. Wang, "An Intrusion Detection Model with Hierarchical Attention Mechanism," IEEE Access, vol. 8, pp. 67542-67554, 2020. https://ieeexplore.ieee.org/document/9098054

[10]. S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," IEEE Access, vol. 7, pp. 42450-42471, 2019. https://ieeexplore.ieee.org/document/8694026

[11]. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6822-6834, Aug. 2019. https://ieeexplore.ieee.org/document/8690688

[12]. Y. Chen, B. Pang, G. Shao, G. Wen, and X. Chen, "DGA-Based Botnet Detection Toward Imbalanced Multiclass Learning," Tsinghua Science and Technology, vol. 26, no. 4, pp. 387-402, Aug. 2021. https://ieeexplore.ieee.org/document/9530501

[13]. X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. S. Rodrigo, "An IoT-Focused Intrusion Detection System Approach Based on Preprocessing Characterization for Cybersecurity Datasets," Sensors, vol. 21, no. 2, p. 656, Jan. 2021. https://www.mdpi.com/1424-8220/21/2 /656

[14]. Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, "Network Intrusion Detection System: A Systematic Study of Machine Learning and Deep Learning Approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, p. e4150, Jan. 2021. https://onlinelibrary.wiley.com/doi/10.1002/ett.4150

[15]. M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. Usman, ‘‘Machine learning classification of port scanning and DDoS attacks: A comparative analysis,’’ Mehran Univ. Res. J. Eng. Technol., vol. 40, no. 1, pp. 215–229, Jan. 2021 https://publications.muet.edu.pk/index.php/muetrj/artcle/view/1999.