Journal of Information Systems Engineering and Management
2025, 10(57s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Machine Learning Approaches for Mitigating Distributed Denial of Service Attacks: A Systematic Review of Advanced Security System

Ms. Priti Chorade[1], Dr. Narendra Chaudhari[2]
Research Scholar, Mansarovar Global University, Bhopal (M.P), India[1]
Professor, Mansarovar Global University, Bhopal (M.P), India[2]

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Distributed Denial of Service (DDoS) attacks are among the most destructive cyber threats. They push so much fake traffic to these sites that they can no longer be reached by real users. It is hard for legacy intrusion detection systems to catch new threats as soon as they arise. This review focuses on how ML helps find DDoS attacks, mainly in SDNs, IoT systems and those used in Agriculture 4.0. Using both supervised, unsupervised and hybrid ML models greatly boosts the accuracy and expands the applications of detection technology. We also review important datasets, different feature engineering solutions and how models perform, giving a full overview of both existing research and upcoming trends.

Keywords: DDoS, Machine Learning, Intrusion Detection, Cybersecurity, Software-Defined Networks, IoT, Feature Engineering

INTRODUCTION

The increasing trust on digital infrastructures has made cyberspace a prime target for malicious activities, among which Distributed Denial of Service (DDoS) attacks remain one of the most disruptive. These attacks flood targeted systems with illegitimate requests, overwhelming their capacity and rendering legitimate access impossible. Traditional intrusion detection systems often fall short in recognizing complex DDoS patterns in real-time due to the evolving sophistication of attack vectors and the use of anonymizing techniques by attackers [1,2].

In the past few years, including machine learning (ML) in information security has been suggested as a good way to protect systems. ML can sort through lots of network traffic data to distinguish good from bad traffic which helps detect threats early and respond automatically [3,4]. Through Deep Neural Networks, Support Vector Machines and ensemble models, ML has been used in Software-Defined Networks (SDNs) and Agriculture 4.0 to reliably point out DDoS attacks with few false signals [5,6].

Most advanced information security systems not only take advantage of machine learning but include tools like feature selection, data preparation and adaptive learning to boost their efficiency and ability to scale [7,8]. Research also points out that using real-world data like CICDDoS2019 helps train and validate these methods for actual use [9].

BACKGROUND OF THE STUDY

Distributed Denial of Service (DDoS) attacks now pose a great danger to digital infrastructure by overwhelming resources with large botnets and disrupting users' ability to connect. Most of the time, these systems cannot catch new or changed attack styles because they are built on limited signatures and fixed rules [11]. To deal with these issues, ML and DL models have aimed to do the learning and pattern detection of attacks themselves while viewing network traffic. For example, deep learning in anomaly-based intrusion detection is effective in handling the changes and new threats in dynamic networks [11]. Using CNNs and RNNs identifies both the shape and the specific timing of the data which is necessary for telling whether behavior is safe or harmful [12].

Many research studies have analyzed and investigated how ML can be applied in cybersecurity. These works tell us that deep learning can greatly improve detection, but there are still difficulties in real-time performance, labeling data and being explained [13]. Besides that, using advanced systems with hybrid, ensemble and feature selection strategies can boost the strength of systems and lower false positive cases [14].

In addition, quantum cryptography and artificial intelligence are now working together with traditional cybersecurity methods, providing new paths for insights into quantum enhanced security systems [15]. Using emerging technologies together with conventional ML frameworks can build DDoS mitigation systems that are strong, flexible and stand firm against attacks.

METHODOLOGY

As this study adopts a systematic review approach, it is essential to outline the methodology employed for selecting and analyzing the literature to ensure transparency and reproducibility.

1. Search Strategy

A large search was done in these academic databases: ScienceDirect, IEEE Xplore, MDPI, SpringerLink and ACM Digital Library. From 2017 to 2025, researchers searched through conference papers, peer-reviewed journal articles and review articles. The search terms included:

- “Distributed Denial of Service” OR “DDoS”
- “Intrusion Detection” OR “Cybersecurity”
- “Machine Learning” OR “Deep Learning”
- “DDoS mitigation” OR “Traffic classification”

2. Study Selection Criteria

Articles were screened based on the following criteria:

- Inclusion Criteria:
    - Focused on ML based approaches for DDoS detection or mitigation.
    - Empirical studies using benchmark or real-world datasets.
    - Reviews or comparative studies analyzing ML models for network security.
    - Published in English between 2017 to 2025.
- Exclusion Criteria:
    - Non-ML-based or purely theoretical DDoS research.
    - Articles lacking experimental validation.
    - Non-peer-reviewed sources (blogs, editorial notes).
    - Duplicate or redundant publications.

1. Selection Process
2. The PRISMA methodology was used to guide the selection process. Initially, 312 articles were identified. After removing 48 duplicates, 264 articles were screened. After reviewing these, 72 full-text articles were assessed for eligibility, resulting in a final selection of 38 studies. The complete PRISMA flow diagram illustrating this process is presented in Figure 1.

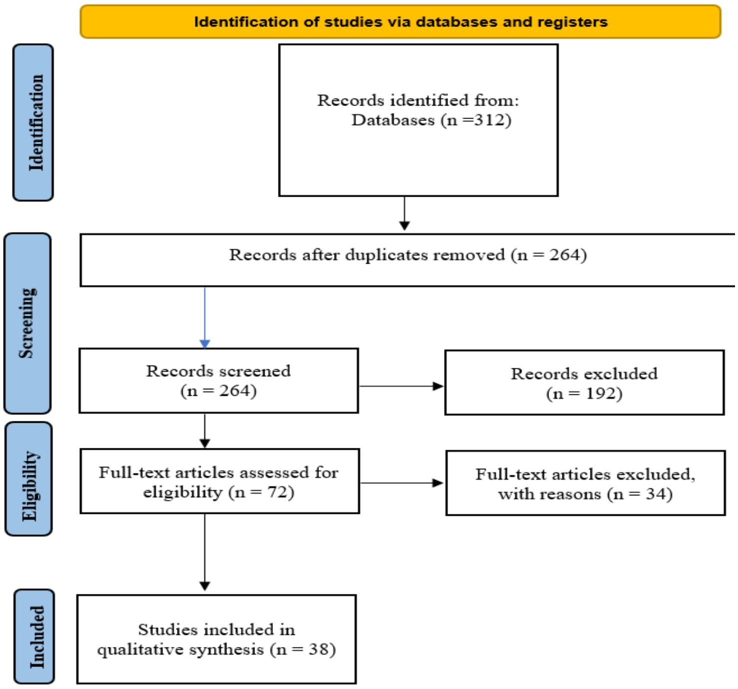
Identification of studies via databases and registers
Identification
Records identified from: Databases (n =312)
Screening
Records after duplicates removed (n = 264)
Records screened (n = 264)
Records excluded (n = 192)
Eligibility
Full-text articles assessed for eligibility (n = 72)
Full-text articles excluded, with reasons (n = 34)
Included
Studies included in qualitative synthesis (n = 38)

Figure 1. PRISMA Flow Diagram Illustrating the Study Selection Process for Systematic Review

4. Bias and Limitations

While every effort was made to ensure objectivity and coverage, the following limitations were acknowledged:

- Selection bias: Limiting sources to English-language and indexed publications may have excluded relevant studies.
- Publication bias: The review may lean toward studies with favorable outcomes or high detection accuracies.

TAXONOMY OF DDOS ATTACKS

Distributed Denial of Service (DDoS) attacks encompass a broad spectrum of techniques aimed at overwhelming target systems with traffic to disrupt availability. A clear taxonomy of these attacks helps in understanding the behavioral characteristics, vectors, and defense requirements of each type. Based on current literature and surveys in intrusion detection, DDoS attacks can be classified into several major categories: volume-based attacks, protocol-based attacks, and application-layer attacks [18,19].

1. Volume-Based Attacks

Volume-based cyber-attacks are designed to overwhelm a target system's bandwidth by flooding it with excessive traffic, commonly through methods like UDP flooding, ICMP flooding, or amplification techniques. These attacks are defined by their high data throughput, typically quantified in bits per second (bps)[19]. In multimedia-focused IoT environments, such attacks are particularly harmful, as they consume substantial bandwidth and significantly degrade service performance[26].

2. Protocol-Based Attacks

Unlike volume-based attacks, protocol attacks focus on exhausting server resources such as connection tables, CPU, or memory, often measured in packets per second (pps) [19, 27]. Protocol-based DDoS attacks are especially challenging to detect in cloud and IoT environments where traffic patterns are highly dynamic [20].

3. Application-Layer Attacks

These are stealthier and more sophisticated, targeting specific features of web applications, such as HTTP, HTTPS, DNS, or SMTP. Examples include HTTP GET/POST floods, Slowloris, and low-and-slow attacks. They are measured in requests per second (rps) and are particularly difficult to detect using conventional threshold-based approaches [18,26]. Enhanced ML/DL models, such as ANN and clustering ensembles, have shown efficacy in detecting these nuanced behaviors [26,27].

4. Distributed Source Variants

A key dimension in DDoS taxonomy is whether the attack originates from a single system or a botnet. Distributed sources make mitigation difficult due to IP spoofing and geographic dispersion. Systems like Botnet-for-hire (DDoS-as-a-Service) have further blurred the lines, allowing unskilled attackers to launch massive attacks with rented infrastructure [19,28].

5. Intelligent and Adaptive Attacks

Recent trends show the rise of adaptive DDoS attacks that learn from target responses and dynamically adjust parameters like attack vector, volume, and timing to evade detection [18,22]. To combat such threats, researchers advocate integrating advanced ML techniques such as ensemble KNN, capsule networks, and decision tree classifiers, which are capable of real-time behavioral adaptation [22-25].

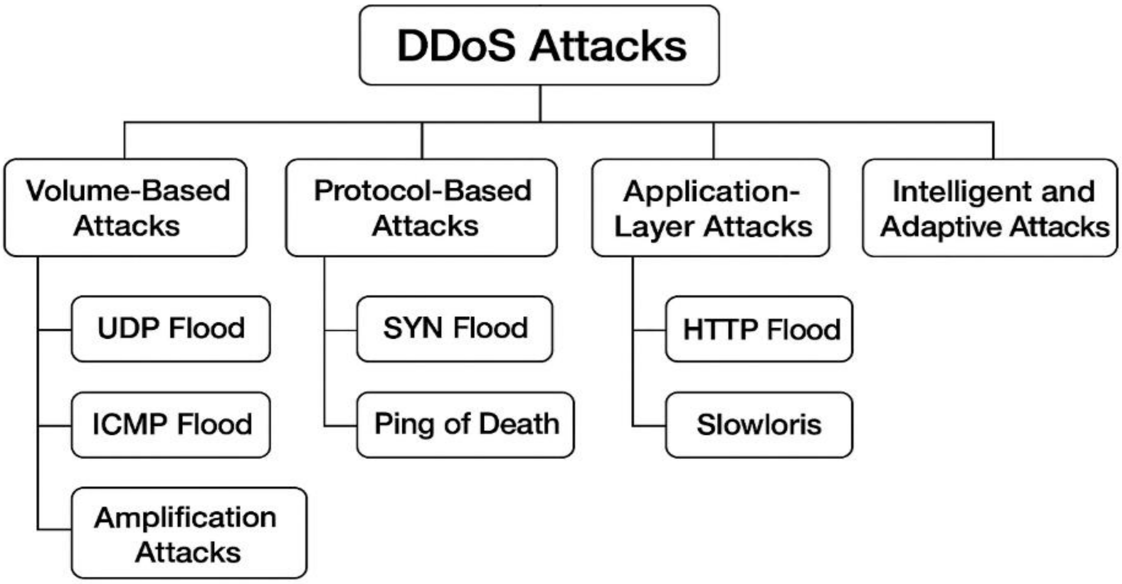

Figure 2. Taxonomy of DDoS Attacks

3. ROLE OF MACHINE LEARNING IN CYBERSECURITY

While security measures such as firewalls and static intrusion detection systems (IDS) have worked well in the past, they cannot adapt and expand as new cyber threats, especially Distributed Denial of Service (DDoS) attacks, emerge. Because of this, cybersecurity professionals are using Machine Learning (ML) more often to handle new and unexpected attacks [26].

Since SVM, Random Forest and Decision Trees are simple to use and effective on labeled datasets, researchers mostly rely on them to detect DDoS attacks. Aljuhani [26] stated that with ANN, they could model traffic behaviors with an accuracy over 97%, proving that deep learning holds impressive potential in traffic modeling. In practice, when these models work with network data, their performance suffers because of noise, uneven data classes and continued mutations of attacks mentioned by Khalaf et al. [27]. This means that, while supervised models do well in specific situations, they only work well for new data if the preprocessing is strong and the models are constantly updated. It appears from new research that using hybrid methods which include both labeled and unlabeled data, allows cybersecurity systems to achieve stability and accuracy as threats and attacks develop over time.

Unsupervised learning techniques, including clustering and autoencoder-based anomaly detection, provide viable alternatives when labeled data is scarce or unavailable. These approaches detect traffic deviations from learned baselines, making them effective for early anomaly detection—even in encrypted or obfuscated traffic [28].

Hybrid and ensemble techniques—such as the combination of decision trees with XGBoost or CNN+RNN stacks—enhance detection robustness by fusing multiple learning perspectives. Qasim and Nsaif [30] demonstrated a hybrid time-series model with improved true positive rates and reduced false alarms, showcasing the growing sophistication of such integrated architectures.

The rise of these intelligent systems is facilitated by the availability of benchmark datasets such as CICDDoS2019, NSL-KDD and BoT-IoT which simulate real-world traffic scenarios. Nonetheless, limitations persist regarding dataset generalizability, feature extraction consistency, and handling of encrypted traffic [31]. Moreover, the opaque decision-making nature of deep learning models, coupled with their vulnerability to adversarial inputs, continues to pose critical research challenges [32].

Table 1. Comparative Analysis of ML Approaches

Ref	Authors	ML Technique	Dataset Used	Accuracy / Performance	Domain
[26]	Aljuhani (2021)	ANN	Custom	~97%	General Networking
[27]	Khalaf et al. (2019)	SVM, RF	NSL-KDD, BoT-IoT	94–98%	Hybrid Defense Models
[29]	Mittal et al. (2023)	LSTM, CNN	CICDDoS2019	>95%	SDN
[30]	Qasim & Nsaif (2024)	Hybrid (Time Series)	Custom	Reduced false alarms	Time-Series Detection
[31]	Ahmed & Atia (2025)	CNN + RNN	Real SDN traffic	96.7%	Software-Defined Networking
[32]	Odusami et al. (2020)	Meta-analysis	Application-layer	Mixed	Web Services/Apps

MACHINE LEARNING MODELS AND ALGORITHMS FOR DDOS DETECTION

Machine Learning (ML) plays a pivotal role in identifying and countering Distributed Denial of Service (DDoS) attacks, thanks to its ability to recognize traffic anomalies and classify threats in real time. Unlike static, rule-based detection systems, ML approaches can dynamically adapt to evolving attack behaviors without relying on fixed signatures. The following section explores widely used ML techniques for DDoS detection, highlighting their strengths and application areas.

1. Supervised Learning Models

Supervised ML techniques are commonly used for DDoS detection as they rely on labeled datasets to learn and classify traffic into normal or attack classes.

- Support Vector Machines (SVM): Known for their robustness in high-dimensional spaces, SVMs are effective in distinguishing between attack and legitimate traffic flows. Al-Qatf et al. [36] enhanced SVM performance by integrating feature extraction methods.
- Random Forests and Decision Trees: These ensemble and tree-based classifiers are widely used for their interpretability and resistance to overfitting. Shen et al. [33] employed a bat-algorithm-enhanced ensemble approach for efficient classification of intrusion attempts.
- Fast Learning Networks (FLN): Ali et al. [34] implemented a FLN combined with Particle Swarm Optimization (PSO) to accelerate learning and improve detection speed in network intrusion scenarios.

2. Feature Engineering and Selection Methods

The effectiveness of ML classifiers depends significantly on the quality of features. Dimensionality reduction and selection techniques are used to improve classifier accuracy and efficiency.

- Stacked Sparse Autoencoders for Feature Extraction: While originally a DL method, their application in preprocessing for traditional classifiers like SVMs is considered ML-enhanced. Yan and Han [35] utilized autoencoders for creating concise feature sets that improved detection precision.
- Optimization-Based Feature Selection: Swarm intelligence and evolutionary algorithms, like PSO and genetic algorithms, are often paired with ML classifiers for selecting the most relevant features, reducing false positives, and improving computational performance.

3. Ensemble Learning and Hybrid Methods

Combining multiple ML algorithms into ensembles often leads to better generalization and accuracy in DDoS detection.

- Ensemble SVM with Rule-Based Models: Marir et al. [37] proposed a hybrid framework using Spark, combining distributed computing with ensemble SVMs for large-scale DDoS traffic classification.
- Voting Classifiers: These aggregate predictions from multiple base learners (e.g., SVM + Random Forest + k-NN) to make final decisions based on majority voting, reducing misclassification.

FEATURE ENGINEERING AND DATASET UTILIZATION

Effective DDoS detection using machine learning hinges on well-curated features and reliable datasets. Feature engineering transforms raw network traffic into structured, relevant attributes that drive the learning process. Meanwhile, the dataset's diversity and labeling quality determine a model’s robustness, especially in dynamic and large-scale network environments.

1. Advances in Feature Engineering

Recent work by Malik and Dutta proposed a multi-stage ML pipeline using the IoT-CIDDS dataset, where they engineered 21 essential features using domain-specific knowledge, improving classification of DDoS attack vectors in smart environments [38]. Similarly, Liu et al. applied feature normalization, correlation filtering, and entropy-based methods in Software-Defined Networks (SDN), showing that these techniques significantly reduced model complexity while boosting detection precision [39].

Zaidi et al. emphasized entropy and granular computing for identifying abnormal bursts in packet flows, enhancing feature discrimination even when traffic patterns were subtle or obfuscated [40]. Further refinement came from Alduailij et al., who used mutual information and Random Forest-based feature importance ranking to discard redundant dimensions and retain only statistically significant attributes [41].

Datasets Commonly Used in ML-Based DDoS Detection

The quality, balance, and real-world applicability of datasets are central to building generalizable ML models. Below is a synthesized review of core datasets used in the literature by findings:

Table 2. Domain-specific datasets are used in DDoS-related ML

Dataset	Source / Origin	Key Features	Noted In
IoT-CIDDS	Malik & Dutta (2023)	Realistic IoT traffic, 21 handcrafted features, labeled flows	[38]
CICDDoS2019	Canadian Institute for Cybersecurity	80+ attack types, volumetric & protocol-based features	Widely used
BoT-IoT	UNSW Canberra	IoT-targeted DDoS traffic, large-scale, includes DoS & data theft	[42]
UNSW-NB15	UNSW Canberra	Rich flow-based data with real and synthetic attack traffic	[43]

IoT-DDoS 2022	Sambangi et al. (2022)	Focused on low- and high-rate attacks in Industry 4.0 setups	[44]
OpenStack Logs	Virupakshar et al. (2020)	Deployment-specific traces in a private cloud for real-time modelling	[45]
CTU-13	Czech Technical Univ.	Botnet-generated traffic with background noise	[46]

CONCLUSION

Machine learning has revolutionized DDoS detection by enabling real-time, adaptive, and high-accuracy solutions. Despite the progress, challenges in dataset diversity, model interpretability, and processing overhead must be addressed. Future research should explore explainable AI, quantum-enhanced security, and automated feature engineering for robust and scalable DDoS mitigation.

REFERENCES

[1] Paffenroth, R. C., & Zhou, C. (2019). Modern machine learning for cyber-defense and distributed denial-of-service attacks. IEEE Xplore.

[2] Gadallah, W. G., & Omar, N. M. (2021). Machine Learning-based Distributed Denial of Service Attacks Detection Technique using New Features in Software-defined Networks. ResearchGate.

[3] Fathima, A., Devi, G. S., & Faizaanuddin, M. (2023). Improving distributed denial of service attack detection using supervised machine learning. ScienceDirect.

[4] Meti, N., Narayan, D. G., & Baligar, V. P. (2017). Detection of distributed denial of service attacks using machine learning algorithms in software defined networks. IEEE Xplore.

[5] Aldhyani, T. H. H., & Alkahtani, H. (2023). Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model. MDPI.

[6] Ramzan, M., Shoaib, M., Altaf, A., Arshad, S., & Iqbal, F. (2023). Distributed denial of service attack detection in network traffic using deep learning algorithm. MDPI.

[7] Ferrag, M. A., Shu, L., Djallel, H., & Choo, K. K. R. (2021). Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. MDPI.

[8] Becerra-Suarez, F. L., Fernández-Roman, I., & Forero, M. G. (2024). Improvement of distributed denial of service attack detection through machine learning and data processing. MDPI.

[9] Seufert, S., & O'Brien, D. (2007). Machine learning for automatic defence against distributed denial of service attacks. Academia.edu.

[10] Van, N. T., Thinh, T. N., & Sach, L. T. (2017). An anomaly-based network intrusion detection system using deep learning. *2017 International Conference on System Science and Engineering (ICSSE)*, Ho Chi Minh City, Vietnam, 210–214.

[11] Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2017). Applying convolutional neural network for network intrusion detection. *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, 1222–1228.

[12] Aldweesh, A., Derhab, A., & Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189, 105124. https://doi.org/10.1016/j.knosys.2019.105124

[13] Wang, Y., Lou, X., Fan, Z., Wang, S., & Huang, G. (2022). Verifiable multi-dimensional (t, n) threshold quantum secret sharing based on a quantum walk. *International Journal of Theoretical Physics*, 61(1), 24. https://doi.org/10.1007/s10773-021-04850-9

[14] Summary: In-Depth Guide to Quantum Artificial Intelligence. (2022). Retrieved from https://www.ai-summary.com/summary-in-depth-guide-to-quantum-artificial-intelligence/

[15] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[16] Aleesa, A. M., Zaidan, B. B., Zaidan, A. A., & Sahar, N. M. (2020). Review of intrusion detection systems based on deep learning techniques: Coherent taxonomy, challenges, motivations, recommendations, substantial

analysis and future directions. *Neural Computing and Applications*, 32, 9827–9858. https://doi.org/10.1007/s00521-019-04566-4

[17] Gamage, S., & Samarabandu, J. (2020). Deep learning methods in network intrusion detection: A survey and an objective comparison. *Journal of Network and Computer Applications*, 169, 102767. https://doi.org/10.1016/j.jnca.2020.102767

[18] Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, 32(1), e4150. https://doi.org/10.1002/ett.4150

[19] Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review. *Internet of Things*, 14, 100365. https://doi.org/10.1016/j.iot.2021.100365

[20] Keele, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (Ver. 2.3). EBSE Technical Report. Keele University.

[21] Costa, V. G., & Pedreira, C. E. (2022). Recent advances in decision trees: An updated survey. *Artificial Intelligence Review*, 1–36. https://doi.org/10.1007/s10462-022-10107-4

[22] Zhang, Y., Cao, G., Wang, B., & Li, X. (2019). A novel ensemble method for k-nearest neighbor. *Pattern Recognition*, 85, 13–25. https://doi.org/10.1016/j.patcog.2018.07.025

[23] Yılmaz, A., Küçüker, A., Bayrak, G., Ertekin, D., Shafie-Khah, M., & Guerrero, J. M. (2022). An improved automated PQD classification method for distributed generators with hybrid SVM-based approach using un-decimated wavelet transform. *International Journal of Electrical Power & Energy Systems*, 136, 107763. https://doi.org/10.1016/j.ijepes.2021.107763

[24] Ren, H., & Lu, H. (2022). Compositional coding capsule network with k-means routing for text classification. *Pattern Recognition Letters*, 160, 1–8. https://doi.org/10.1016/j.patrec.2022.06.009

[25] Gopi, R., Sathiyamoorthi, V., Selvakumar, S., Manikandan, R., Chatterjee, P., Jhanjhi, N. Z., & Luhach, A. K. (2022). Enhanced method of ANN based model for detection of DDoS attacks on multimedia internet of things. *Multimedia Tools and Applications*, 81, 26739–26757. https://doi.org/10.1007/s11042-022-12911-0

[26] Aljuhani, A. (2021). *Machine learning approaches for combating distributed denial of service attacks in modern networking environments*. IEEE Access. https://ieeexplore.ieee.org/abstract/document/9366480/

[27] Khalaf, B. A., Mostafa, S. A., & Mustapha, A. (2019). *Comprehensive review of artificial intelligence and statistical approaches in distributed denial of service attack and defense methods*. IEEE Access. https://ieeexplore.ieee.org/abstract/document/8692706/

[28] Kaur, P., Kumar, M., & Bhandari, A. (2017). *A review of detection approaches for distributed denial of service attacks. Journal of Cyber Security Technology*, 1(3–4), 121–138. https://www.tandfonline.com/doi/pdf/10.1080/21642583.2017.1331768

[29] Mittal, M., Kumar, K., & Behal, S. (2023). *Deep learning approaches for detecting DDoS attacks: A systematic review. Soft Computing*. https://link.springer.com/article/10.1007/s00500-021-06608-1

[30] Qasim, S. S., & Nsaif, S. M. (2024). *Advancements in time series-based detection systems for distributed denial-of-service (DDoS) attacks: A comprehensive review. Basrah Journal of Networks*. https://mesopotamian.press/journals/index.php/BJN/article/view/255

[31] Ahmed, R. S., & Atia, T. S. (2025). *Machine learning and deep learning for distributed denial of service attack detection in software-defined networking: A review. AIP Conference Proceedings*. https://pubs.aip.org/aip/acp/article-abstract/3211/1/030030/3346061

[32] Odusami, M., Misra, S., & Abayomi-Alli, O. (2020). *A survey and meta‐analysis of application‐layer distributed denial‐of‐service attack. International Journal of Communication Systems*, 33(18). https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4603

[33] Shen, Y., Zheng, K., Wu, C., Zhang, M., Niu, X., & Yang, Y. (2018). An ensemble method based on selection using bat algorithm for intrusion detection. *Computer Journal*, 61(4), 526–538. https://doi.org/10.1093/comjnl/bxx054

[34] Ali, M.H., Al Mohammed, B.A.D., Ismail, A., & Zolkipli, M.F. (2018). A new intrusion detection system based on fast learning network and particle swarm optimization. *IEEE Access*, 6, 20255–20261. https://doi.org/10.1109/ACCESS.2018.2827553

[35] Yan, B., & Han, G. (2018). Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. *IEEE Access*, 6, 41238–41248. https://doi.org/10.1109/ACCESS.2018.2854186

[36] Al-Qatf, M., Lasheng, Y., Al-Habib, M., & Al-Sabahi, K. (2018). Deep learning approach combining sparse autoencoder with SVM for network intrusion detection. *IEEE Access*, 6, 52843–52856. https://doi.org/10.1109/ACCESS.2018.2872784

[37] Marir, N., Wang, H., Feng, G., Li, B., & Jia, M. (2018). Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using Spark. *IEEE Access*, 6, 59657–59671. https://doi.org/10.1109/ACCESS.2018.2875865

[38] Malik, M., & Dutta, M. (2023). Feature engineering and machine learning framework for DDoS attack detection in the standardized internet of things. *IEEE Internet of Things Journal*. https://ieeexplore.ieee.org/abstract/document/10044970/

[39] Liu, Z., Wang, Y., Feng, F., Liu, Y., Li, Z., & Shan, Y. (2023). A DDoS detection method based on feature engineering and machine learning in software-defined networks. *Sensors*, 23(13), 6176. https://www.mdpi.com/1424-8220/23/13/6176

[40] Aamir, M., & Zaidi, S.M.A. (2019). DDoS attack detection with feature engineering and machine learning: The framework and performance evaluation. *International Journal of Information Security*, 18, 425–448. https://link.springer.com/article/10.1007/s10207-019-00434-1

[41] Alduailij, M., Khan, Q.W., Tahir, M., Sardaraz, M., & Alduailij, M. (2022). Machine-learning-based DDoS attack detection using mutual information and random forest feature importance method. *Symmetry*, 14(6), 1095. https://www.mdpi.com/2073-8994/14/6/1095

[42] Panda, M., Abd Allah, A.M., & Hassanien, A.E. (2021). Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber attacks. *IEEE Access*, 9, 84435–84450. https://ieeexplore.ieee.org/abstract/document/9464257/

[43] Karatas, G., Demir, O., & Sahingoz, O.K. (2020). Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset. *IEEE Access*, 8, 32150–32162. https://doi.org/10.1109/ACCESS.2020.2973218

[44] Sambangi, S., Gondi, L., & Aljawarneh, S. (2022). A feature similarity machine learning model for DDoS attack detection in modern network environments for Industry 4.0. *Computers & Electrical Engineering*, 101, 107877. https://www.sciencedirect.com/science/article/pii/S0045790622002324

[45] Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S., & Narayan, D.G. (2020). Distributed Denial of Service (DDoS) attacks detection system for OpenStack-based private cloud. *Procedia Computer Science*, 167, 2297–2307. https://doi.org/10.1016/j.procs.2020.03.281

[46] Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability*, 12(3), 1035. https://www.mdpi.com/2071-1050/12/3/1035

[47] Maslan, A., & Mohamad, K.M.B. (2020). Feature selection for DDoS detection using classification machine learning techniques. *Seminar Nasional Teknologi Informasi dan Komunikasi Terapan (SENTIKA)*. https://pdfs.semanticscholar.org/65cb/c64e4e2ab302a7e43e430d49172a90045632.pdf

[48] Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability*, 12(3), 1035. https://www.mdpi.com/2071-1050/12/3/1035