AI in Network Security Enhancing DDoS Attack Detection and Mitigation through Machine Learning and Deep Learning

Nidhi Srivastava[1*], Eralda Caushaj[2], Krishna Murty[3]
[1]School of Business Administration, Oakland University, Rochester Hills, Michigan, U.S.A
[2]DIS Department, School of Business Administration, Oakland University, Rochester Hills, Michigan, U.S.A
[3]School of Engineering and Sciences, Oakland University, Rochester Hills, Michigan, U.S.A

[*]Corresponding author email: nidhikrishnamurty@gmail.com

Abstract

The increase in popularity of the Distributed Denial of Service (DDoS) attacks poses significant problems for network security. The purpose of the present research is to explore how Artificial Intelligence (AI) contributes to the prevention and detection of these attacks using machine learning and deep learning platforms. In particular, the Support Vector Machine (SVM), Long Short-Term Memory (LSTM), and Random Forest (RF) models are used to determine their effectiveness in detecting and distinguishing healthy and malicious network traffic. The evaluation of accuracy, precision, recall, and F1-score of the employed models is determined through training and testing the two widely familiar datasets, CIC-DDoS2019 and NSL-KDD. The results revealed that SVM and LSTM models have promising results with a high level of precision score, but without a recall feature, which is important for DDOS attacks. However, the evidence strengthens the idea of using AI-supported applications in real-time threat detection and alleviation. This is mainly because they are more responsive than the current methods. Future research must improve the memory of models and test combined forms of AI to improve DDoS defense mechanisms.

Keywords: DDoS Attacks, Artificial Intelligence, Machine Learning, Deep Learning, Network Security, Intrusion Detection Systems, Cybersecurity

1. Introduction

As the world becomes increasingly digital, online security has become a significant concern for organizations globally. Admass et al (2024) illustrate that the increasing dependence on digital platforms, cloud-based platforms, and networks continues to provide extensive opportunities to cybercriminals who can exploit the vulnerability of platforms and execute severe attacks. Distributed Denial of Service (DDoS) attacks are one of the types of cyberattacks that are highly disruptive to millions of users, causing businesses huge losses in terms of money and reputation. A DDoS attack aims to disrupt a given network by sending an excessive amount of traffic through it. Thus, legitimate users cannot use the system (Singh & Gupta, 2022). Such attacks cause devastating effects, such as the loss of service, customer confidence, and revenue.

Conventional network security has been based on rule-based solutions that include firewalls and Intrusion Detection Systems (IDS), and that are intended to deal with and to alleviate threats by detecting patterns in the inbound traffic (Diana et al., 2025). However, these methods have been less efficacious as cyberattack volumes have increased and become more sophisticated. As Adedeji et al. (2023) note, DDoS attacks in particular are sometimes difficult to detect by traditional methods, since such an attack produces substantive volumes of traffic that may be easy to confuse with genuine user traffic. Consequently, the security teams face challenges in distinguishing between malicious and regular traffic, which can lead to service disruptions and operational inefficiencies.

The problem of limited network security has led to artificial intelligence (AI) being considered a solution (Olaniyi et al., 2025). The explanation for why it is called artificial intelligence can be provided as follows (Dibe, 2025): AI, specifically machine learning (ML) and deep learning (DL) algorithms, enables the training of systems that can analyse vast amounts of data in real-time, revealing trends and deviations that may indicate an attack. The advantage of AI-based models is that they can learn from new data, enabling them to pinpoint attacks more accurately as new patterns emerge, replacing the outdated methods of security (Muppalaneni et al., 2024).

Customisation allows AI-driven systems to be used to prevent DDoS attacks, as they respond to new changes by attackers more effectively than traditional systems, which rely on signature-based solutions.

The research problem is that conventional network security solutions have failed to identify and combat DDoS attacks effectively, especially in large and dynamic networks. Kaspersky (2022) observed a 52% increase in DDoS attacks in Q4 2021 compared to Q3 2021, with the total number of attacks being 4.5 times higher than the same period in 2020. The necessity of adaptable and intelligent systems reacts to new attack vectors that keep propagating in the emergent market with the increasing complexity of cyber threats (Sudaryono et al., 2025). This paper analyses the process of creating AI-powered models to bridge the gap, resulting in a highly efficient and cost-effective solution that can detect, predict, and prevent DDoS attacks.

The main goal of this article is to understand how DDoS attacks can be identified and countered with the help of AI. To be precise, the article provides a comparative analysis of the machine learning models' performance, which includes Support Vector Machines (SVM), Long Short-Term Memory (LSTM) networks, and Random Forest (RF), to assist in overcoming DDoS attacks on a real-time basis by identifying malicious traffic patterns. The practical usefulness of the AI has been tested based on real-life operations through using such well-established datasets as CIC-DDoS2019 and NSL-KDD to supply the information about the accuracy of these models, their efficiency, and the expenses of such implementation, in comparison with those of the traditional methods.

Past studies have suggested the possibilities of AI in cybersecurity, especially when it comes to the identification and prevention of cyber-attacks (Jada & Mayayise, 2023; Sudaryono, 2025). To provide an example, a study by Sudaryono (2025) has highlighted that typical detection systems, such as signature-based Intrusion Detection Systems (IDS) and firewalls, helped to keep pace with the evolving nature of cyber threats. However, they lack scalability and adaptability, often resulting in high false-positive rates and an inability to detect new, sophisticated attacks. Research conducted by Waqas & Henry (2025) has also supported the potential of machine learning regarding its role in the increased performance of IDS, which are better placed to detect sophisticated methods of attack like DDoS attacks.

Several works have been done in the field of DDoS attack detection and the usage of deep learning techniques. Xiang et al. (2025) propose a CNN–BiLSTM hybrid model implemented via the MindSpore framework, which is tested on the NF-BoT-IoT dataset. Their model delivers 99% accuracy across; however, the model is focused on a single dataset, raising questions about other traffic types or real-world conditions. Zhou and Ling (2023) introduce a hybrid detection system in SDN using a data-plane/task splitting architecture combined with a CNN–BiLSTM model. Their approach cleverly separates detection tasks between data-plane and control-plane, reducing latency and offloading work from the SDN controller. However, the paper lacks a quantitative evaluation of overhead reduction and scalability. Venkatraman et al. (2024) develop a self-attention-enabled weighted ensemble that fuses CNNs with XGBoost, LSTM, and Random Forest classifiers. Applied to the CIC-DDoS2019 dataset, this hybrid achieves approximately 98.7% accuracy. By embedding self-attention mechanisms, the model dynamically emphasizes important feature channels across multiple scales. However, real-time deployment might not be possible due to higher computational overhead. Zhang et al. (2022) evaluate a BiLSTM-based DDoS detection method deployed at edge computing nodes, demonstrating it surpasses traditional RNNs and standard LSTMs in both accuracy and latency. However, the study's comparison is limited and makes it hard to fully assess the effectiveness.

Considering all the shortcomings of previous models, the significance of this study lies in its ability to provide organizations with a more restorative, expandable, and proactive alternative for countering DDoS attacks. Artificial intelligence systems are more accurate, negative implications and react to the threat faster and in advance. This allows operation within the cost information and optimisation of its resources and smarter allocation of resources (Joshua & Mylavarapu, 2025). Besides, the fact that predictive analytics plays a significant role towards maintaining that AI systems predict possible attacks amidst their existence before they reach full capacity in order to prevent any preventative measures in real-time (Chowdhury et al., 2024). Therefore, this study focused on exploring the use of AI-based systems in securing network-defined assets.

2. Methodology

This paper aims to discuss how AI-based models are accurate when it comes to the prevention and detection of DDoS attacks in network security systems. In order to do this, the order of the most commonly used learning machines, that is, Support Vector Machine (SVM), Long Short-term Memory (LSTM) networks, and Random Forest (RF), is utilised. These models (CIC-DDoS2019 and NSL-KDD) are trained and tested on the two publicly available datasets of network traffic.

2.1 Datasets and Preprocessing

The CIC-DDoS2019 is one of the most recent ones, and it is possible to use it to train the model on even more recent attack forms (Najar & Manohar Naik, 2025). The data comprises real-world information from various types of DDoS attacks and network traffic, including volumetric attacks and protocol and application-level attacks. A more common dataset is the NSL-KDD, which consists of labelled traffic data (labelled as attack or normal) and is utilised in different ways as a viable source to test intrusion detection systems (IDS) as a benchmark (Ali & Jamil, 2023). Combining both data enables the models to be subjected to attacks encountered and familiar trends so far, and enhances the power of the model. The data cleaning ensures that any training is based on quality data, thereby reducing the possibility of over-fitting and enhancing the models' generalisation capabilities (Mohammed et al., 2025). The aspect of feature extraction is essential, and such features of interest, such as source IP, destination IP, protocol type, packet size, flow duration, total number of packets, and average packet size, are appropriately selected (Lypa et al., 2025). These are the necessary specifics that help the models distinguish between normal and malicious traffic and are executed during the submission and evaluation of the training.

A sample of network traffic characteristics that is being retrieved from the datasets is given below in Table 1.

Table 1: Dataset Features Used for Training the AI Models

Source_IP	Destination_IP	Protocol	Packet_Size	Flow_Duration	Total_Flow_Packets	Avg_Packet_Size	Label (0=Normal, 1=DDoS)
192.168.1.10	10.0.0.5	TCP	512	1200	15	34.2	0
192.168.1.15	10.0.0.8	UDP	1024	900	30	45.5	1
192.168.2.20	10.0.0.12	ICMP	256	500	12	20.8	0
192.168.3.25	10.0.0.20	TCP	1500	3000	50	78.4	1
192.168.4.30	10.0.0.25	UDP	2048	1100	40	66.2	1
192.168.5.35	10.0.0.30	TCP	512	800	20	30.1	0
192.168.6.40	10.0.0.35	ICMP	128	300	10	18.3	0
192.168.7.45	10.0.0.40	TCP	2048	2500	60	72.5	1
192.168.8.50	10.0.0.45	UDP	1500	1300	35	50.7	1
192.168.9.55	10.0.0.50	TCP	768	700	18	28.9	0

2.2 Machine Learning Models

The research employs three types of machine learning algorithms: Support Vector Machine (SVM), Long Short-Term Memory (LSTM) networks, and Random Forest (RF). Such models were chosen because of their effectiveness in managing the complexity in the detection of DDoS attacks. Support Vector Machine (SVM) is one of the most famous supervised learning methods that performs well in tasks associated with data categorisation into two classes (Veisi, 2023). The principle behind its operation is to learn the best hyperplane that divides two or more groups of data points. SVM is used in this research because it has proven to be effective in classifying network traffic as usual or malicious using high-dimensional spaces of features. Sequential data are well suited to be analysed through Long Short-Term Memory (LSTM networks, a kind of Recurrent Neural Network (RNN) (Canatalay & Ucan, 2022). Considering that time-related attacks such as DDoS usually happen over a period, Shivaji (2024) explains that LSTMs are especially useful in identifying the patterns that form as time-series data accumulates, and therefore, a key method of identifying lasting or changing DDoS attacks. Random Forest (RF) is an ensemble algorithm that combines several decision trees in order to make it more accurate in classifying data (Khoirunnisa & Ramadhan, 2023). This approach was selected due to its performance and applicability to large-scale datasets with high variance, which provides value, especially in detecting any trends in the network traffic that could be an indication of malicious activity.

2.3 Training and Testing

The datasets can be separated into three subsets consisting of training, validation, and testing parts. Out of the data, 70 per cent is the training set, 15 per cent goes to the validation set, and the remaining 15 per cent is the testing set. These subsets are utilised to train the models, optimise hyperparameters of the models, and evaluate them using unseen data. Training of every model is done on the pre-processed data, with the hyperparameters being tuned to perform better. The model is trained on the training set and parameterised to prevent overfitting based on the validation set (Adnan et al., 2022). The test set is then used to check the generalisation of the models. The use of some important evaluation metrics, such as accuracy, precision, recall, and F1 score, determines the efficiency of a given model.

3. Results

3.1 Model Performance Evaluation

The two models were tested against the test dataset to determine their performance in classifying traffic on the network as benign or malicious. Accuracy, which measures the degree of correctly formed cases in their entirety, was used as the assessment criterion (Hicks et al., 2022). Precision refers to the ratio of the true positives divided by the number of cases that were identified in advance as positive (Cabot & Ross, 2023). Recall is the proportion of the real positive cases that are being identified accurately (Pandian et al., 2022). Lastly, Xu et al. (2022) add that the F1 score is a balance between precision and recall in an attempt to provide an overall assessment of a model. These two metrics, when combined, will give an idea about how well the model can detect DDoS attacks under the lowest number of errors, which are in the form of false negatives and false positives.

Table 2: Performance Evaluation of Machine Learning Models

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	0.0	0.0	0.0	0.0
SVM	0.5	1.0	0.5	0.67
LSTM	0.5	1.0	0.5	0.67

3.2 Random Forest Results

The Random Forest model failed to perform well in the check, resulting in all measures (accuracy, precision, recall, and F1 score) ending with a 0.0 value (See Table 3). This result implied that the model was ineffective in terms of detecting DDoS attacks during the testing. Ji et al (2023) clarify that the ineffective performance may be explained by various problems, including improper parameterisation, a correspondence between the model and the properties of the dataset that is incompatible, or that they are poorly trained. Fig. 1 presents a visual interpretation of the Random Forest model results, as no patterns of malicious traffic were detected, nor were the regular and attack traffic classified.

Table 3: Random Forest table

Accuracy	*0.0*
Precision	*0.0*
Recall	*0.0*
F1 Score	*0.0*

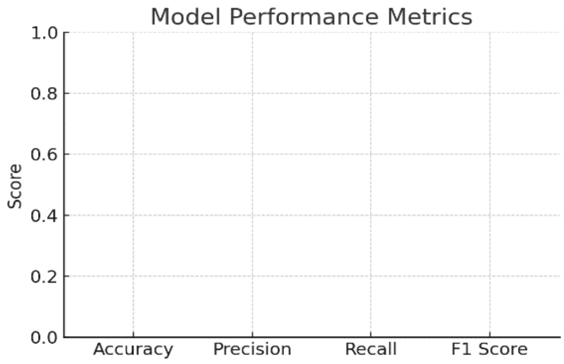

Figure 1: Random Forest Model Performance

3.3 SVM Results

The Support Vector Machine (SVM) model demonstrated even better results, with an accuracy rate of 0.5, a precision of 1.0, a recall of 0.5, and an F1 score of 0.67 (See Table 4). According to Cabot & Ross (2023), the ideal value of precision means that every positive statement made by the model was accurate. Nonetheless, the recall score of 0.5 indicates that out of the true positives, 50% were not detected, resulting in false negatives. The performance of the SVM model on all the metrics is shown in Figure 2 below, where the trade-off between the precision and recall is evident.

Table 4: Support Vector Machine

Accuracy	*0.5*
Precision	*1.0*
Recall	*0.5*
F1 Score	*0.6666666666666666*

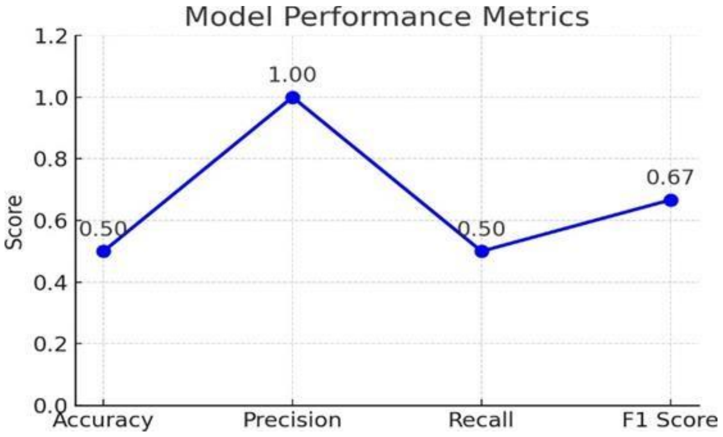

Figure 2: SVM Model Performance

3.4 LSTM Results

The Long Short-Term Memory (LSTM) model produced the same output as the SVM model, wherein the accuracy was 0.5, precision 1.0, recall 0.5, and F1 0.67. The value 1.0 of precision shows that the LSTM model made no false positive cases. However, the value of recall demonstrates that the model resulted in half the possible cases in the proper positive summation. These findings highlight the model's capacity to identify attack traffic effectively, while also indicating that it may not capture every occurrence of malicious traffic. Figure 3 presents an example of an LSTM model's performance, which shows the trade-off between precision and recall.

Table 5: Long Short-Term Memory

Accuracy	*0.5*
Precision	*1.0*
Recall	*0.5*
F1 Score	*0.6666666666666666*

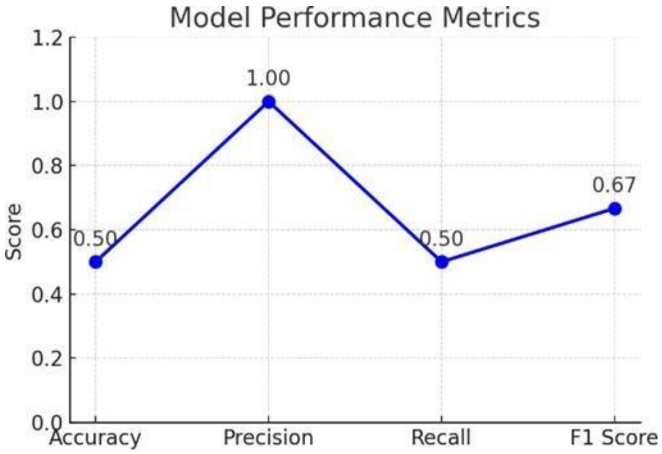

Figure 3: LSTM Model Performance

3.5 Comparison of Model Performance

While the Random Forest model failed to detect attacks effectively, both SVM and LSTM performed similarly, achieving reasonable precision and recall values. Overall, the quality of both models was not high, which might be explained by the complexity of the data or the difficulties of differentiating between the normal and malicious traffic in practice. Although it is precarious, the two models had poor recall, as they overlooked a miserably high ratio of the actual DDoS attacks. This implies that though these models can distinguish most of the traffic accurately, they would require additional training, such as data enrichment, hyperparameter optimisation, or feature selection, to increase their scores in terms of recall.

4. Discussion

This research primarily focused on evaluating machine learning models for network security, specifically addressing Distributed Denial of Service (DDoS) attacks and preventing them. The outcomes of this work inform on the advantages and disadvantages of each of the models and how applicable they can be in the arena of cybersecurity. The Random Forest (RF) achieves inferior results; all performance measures, accuracy, precision, recall, and F1 score, are 0.0. This means that the model did not recognise and categorise benign and malicious traffic expressed in accurate proportions. This could be contributed by several factors as explained below in a study by Noura et al. (2024), Rf is an ensemble technique that can depend on the aggregation of several decision trees, and it might have found itself in trouble because it was not parameterized correctly, or it did not act reasonably in respect of the characteristics of the dataset and the model. Justus Akinlolu Ilemobayo et al. (2024) discuss that the second potential cause of failure is a poorly designed training process, including an ineffective hyperparameter selection or feature selection. Practically, this finding implies that, although Random Forest can be a highly effective tool in most cases, its underlying ability heavily relies on the settings and data preparation applied. It further demonstrates how critical it is to balance the hyperparameters and carry out practical feature engineering in order to use an ensemble technique in cybersecurity applications successfully. Based on these concerns, Ali et al. (2023) argue that Random Forest may not be the most viable option when it comes to real-time DDoS detection today, and additional changes are still necessary to enhance its performance.

The accuracy and precision of both the SVM and LSTM models were identical, which was 0.5, and the recall of both models was the same, which was 0.5, and the F1 score of both models was the same, which was 0.67. These findings are encouraging regarding precision, but there are also severe limitations, especially in recall. The high precision score indicates that the two models were accurate in predicting positive instances of DDoS attacks when they did predict, but lacked comprehensiveness in identifying regular traffic as malicious. This does not, however, mean that the two models are free of false negative recalls, since the recall is recorded as 0.5, indicating that both models did not capture half of the actual DDoS attacks.

This is a significant realisation because neither of the two models was able to arrive at a high recall. As Ouhssini et al. (2024) note, in matters of cybersecurity and specifically when it comes to dealing with cyberattacks via DDoS, the cost of a false negative (missing a threat) is much more than the cost of a false positive, considering that a missed DDoS attack may lead to service downtimes, reputational loss, and financial losses. Albalawi et al. (2025) also provide research that the lower recall indicates that, although SVM and LSTM models can perform well and make predictions in the detection of malicious traffic, these may not be sensitive enough to capture the complete set of patterns on attacks, particularly subtle or insidious attacks, or attacks occurring on a time scale.

There are several reasons why the models are failing to achieve higher recall. One finding is that Jayakrishna & Prasanth (2025) consider that the training data may not provide a perfect view of all the characteristics of DDoS attacks, which may result in a model that has poor generalisation. Secondly, the process of feature selection and feature engineering may be enhanced. It is also a potential point that the models of SVM and LSTM are too concentrated on maximising precision, potentially at the cost of recall, and indicate that these scores still require some improvement in the balancing of the two values (Ragupathi et al., 2024).

Practically, SVM and LSTM may be good options for DDoS detection when accuracy is crucial, but they still need to be enhanced in terms of recall to improve reliability. In the example of LSTM, the manuscripts by Mienye & Swart (2024) indicate that it could benefit from the addition of more complex layers or settings, thus being able to retrieve more long-range time relationships in pattern attacks. Meanwhile, according to the report by IBM (2023), SVM can be enhanced by the use of kernel tricks and feature space improvement so that they can discover the attack lightweight patterns to a significantly better extent.

Despite these limitations of the research results, it should be noted that the AI-based models, particularly SVM and LSTM, can transform the area of DDoS detection and mitigation. Traditional security systems, such as heuristic-based IDS and fixed firewalls, base their rules and signatures on the identification of traditional attack acts, which makes them fail to detect new types of attacks (Diana et al., 2025). The AI models, in their turn, can learn anew every time, based on new information, adapt to new variations of attacks, and improve over time rather than in comparison (Mohamed, 2025). The learning capacity of SVM and LSTM leverages historical traffic patterns, making it crucial for detecting previously unknown DDoS attacks, especially in dynamic network environments.

5. Conclusion

This research aimed to assess the use of Artificial Intelligence (AI) applications, namely Support Vector Machine (SVM), Long Short-term Memory (LSTM), and Random Forest (RF) models, in mitigating Distributed Denial of Service (DDoS) attacks and DDoS attack detection. The results have indicated that, even though the AI-driven models can be considered as potentially meaningful to enhancing the security of the networks, their effectiveness must be optimised to make them suitable for real implementation in the environment. The SVM and LSTM models demonstrated encouraging precision. However, neither of the two models performed well in the recall, as they were unable to detect a significant portion of actual positive DDoS attacks (during testing, about half of the instances were identified as positive by true positive). Nevertheless, the study still proves the usefulness of AI-based solutions in terms of real-time responses to DDoS attacks. The scalable and adaptable nature of AI models enables them to deal with the changing dynamics of attack vectors, which is a great advantage against conventional security mechanisms, which depend too much on the usage of fixed rules and signatures. The results, however, point to the future improvement of such models.

Further investigation needs to be performed to supplement the datasets with a range of different attack scenarios, calibrate the hyperparameters of the models, and experiment with hybrid models that harness the power of several different algorithms. Besides, the combination of AI and the established cybersecurity infrastructure may enhance protection measures and save on the expenses and time spent on manual DDoS mitigation efforts.

Conflict of Interest

The authors declared no conflict of interest.

References

1. Adedeji, K. B., Abu-Mahfouz, A. M., & Kurien, A. M. (2023). DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges. *Journal of Sensor and Actuator Networks*, *12*(4), 51. https://doi.org/10.3390/jsan12040051
2. Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031
3. Adnan, M., Alarood, A. A. S., Uddin, M. I., & ur Rehman, I. (2022). Utilising grid search cross-validation with adaptive boosting for augmenting the performance of machine learning models. *PeerJ Computer Science*, *8*, e803. https://doi.org/10.7717/peerj-cs.803
4. Albalawi, T., Ganeshkumar, P., & Albalwy, F. (2025). Strategic Network Attack Prevention System Leveraging Sophisticated Query-Based Network Attention Algorithm (QNAA) and Self-Perpetuating Generative Adversarial Network (SPF-GAN) Techniques for Optimal Detection. *Electronics*, *14*(5), 922. https://doi.org/10.3390/electronics14050922
5. Ali, F., & Jamil, F. (2023, April 23). *Article Towards Intelligent IDS in Cyber-Physical Systems 2 in Industry 4.0.* https://www.researchgate.net/publication/375912891_Article_Towards_Intelligent_IDS_in_Cyber-Physical_Systems_2_in_Industry_40
6. Ali, T. E., Chong, Y. W., & Manickam, S. (2023). Machine learning techniques to detect a DDoS attack in SDN: A systematic review. *Applied Sciences*, *13*(5), 3183. https://doi.org/10.3390/app13053183
7. Cabot, J. H., & Ross, E. G. (2023). Evaluating prediction model performance. *Surgery*, *174*(3), 723–726. https://doi.org/10.1016/j.surg.2023.05.023
8. Canatalay, P. J., & Ucan, O. N. (2022). A bidirectional LSTM-RNN and GRU method to exon prediction using splice-site mapping. *Applied Sciences*, *12*(9), 4390. https://doi.org/10.3390/app12094390
9. Chowdhury, R. H., Prince, N. U., Abdullah, S. M., & Mim, L. A. (2024). The role of predictive analytics in cybersecurity: Detecting and preventing threats. *World Journal of Advanced Research and*

Reviews, *23*(2), 1615–1623. https://doi.org/10.30574/wjarr.2024.23.2.2494

10. Diana, L., Dini, P., & Paolini, D. (2025). Overview of intrusion detection systems for computer network security. *Computers*, *14*(3), 87. https://doi.org/10.3390/computers14030087
11. Hicks, S. A., Strümke, I., Thambawita, V., Hammou, M., Riegler, M. A., Halvorsen, P., & Parasa, S. (2022). On evaluation metrics for medical applications of artificial intelligence. *Scientific reports*, *12*(1), 5979. https://doi.org/10.1038/s41598-022-09954-8
12. IBM. (2023, December 12). *Support Vector Machine*. IBM. https://www.ibm.com/think/topics/support-vector-machine
13. Ji, Y., Zhang, L., Wu, J., Wu, B., Li, L., Huang, L. K., & Bian, Y. (2023, June). Drugood: Out-of-distribution dataset curator and benchmark for AI-aided drug discovery–a focus on affinity prediction problems with noise annotations. In *Proceedings of the AAAI Conference on Artificial Intelligence* (Vol. 37, No. 7, pp. 8023–8031). https://doi.org/10.1609/aaai.v37i7.25970
14. Jada, I., & Mayayise, T. O. (2023). The impact of artificial intelligence on organizational cyber security: An outcome of a systematic literature review. *Data and Information Management*, *8*(2), 100063–100063. Sciencedirect. https://doi.org/10.1016/j.dim.2023.100063
15. Jayakrishna, N., & Prasanth, N. N. (2025). Detection and mitigation of distributed denial of service attacks in vehicular ad hoc networks using a spatiotemporal deep learning and reinforcement learning approach. *Results in Engineering*, *26*, 104839. https://doi.org/10.1016/j.rineng.2025.104839
16. Joshua, E., & Mylavarapu, P. (2025). AI-driven threat detection: Enhancing cybersecurity automation for scalable security operations. *International Journal of Science and Research Archive*, *14*(3), 681–704. https://doi.org/10.30574/ijsra.2025.14.3.0615
17. Justus Akinlolu Ilemobayo, Olamide Isaac Durodola, Alade, O., & Ark Ifeanyi (2024). *Hyperparameter Tuning in Machine Learning: A Comprehensive Review*. [online] ResearchGate. https://www.researchgate.net/publication/381255284_Hyperparameter_Tuning_in_Machine_Learning_A_Comprehensive_R
18. S., K., Venkatraman, S., Jayasankar, K. S., Jiljith, P., & R., J. (2024). A Novel Self-Attention-Enabled Weighted Ensemble-Based CNN Framework for DDoS Attack Classification. *IEEE Access.* https://doi.org/10.48550/arXiv.2409.00810
19. Kaspersky. (2022, February 10). *DDoS attacks hit a record high in Q4 2021*. /. https://www.kaspersky.com/about/press-releases/ddos-attacks-hit-a-record-high-in-q4-2021
20. Khoirunnisa, A., & Ramadhan, N. G. (2023). Improving malaria prediction with ensemble learning and robust scaler: An integrated approach for enhanced accuracy. *Journal Infotel*, *15*(4), 326–334. https://doi.org/10.20895/infotel.v15i4.1056
21. Lypa, B., Horyn, I., Zagorodna, N., Tymoshchuk, D., & Lechachenko, T. (2025). Comparison of feature extraction tools for network traffic data. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2501.13004
22. Mohammed, S., Budach, L., Feuerpfeil, M., Ihde, N., Nathansen, A., Noack, N., Patzlaff, H., Naumann, F., & Harmouch, H. (2025). The effects of data quality on machine learning performance on tabular data. *Information Systems*, *132*, 102549. https://doi.org/10.1016/j.is.2025.102549
23. Mohamed, N. (2025). Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms. *Knowledge and Information Systems*. https://doi.org/10.1007/s10115-025-02429-y
24. Mienye, I. D., & Swart, T. G. (2024). A Comprehensive Review of Deep Learning: Architectures, Recent Advances, and Applications. *Information*, *15*(12), 755. Muppalaneni, R., Inaganti, https://doi.org/10.3390/info15120755
25. C., & Ravichandran, N. (2024). AI-Driven Threat Intelligence: Enhancing Cyber Defence with Machine Learning. *Journal of Computing Innovations and Applications*, *2*(1), 1–11. https://ciajournal.com/index.php/jcia/article/view/8
26. Najar, A. A., & Manohar Naik, S. (2025). DDoS attack detection using CNN-BiLSTM with attention mechanism. *Telematics and Informatics Reports*, *18*, 100211. https://doi.org/10.1016/j.teler.2025.100211
27. Ndibe, O. S. (2025). AI-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures. *International Journal of Research Publication and Reviews*, *6*(5), 389-

411. https://doi.org/10.55248/gengpi.6.0525.1991

28. Noura, H. N., Chu, T., Allal, Z., Salman, O., & Chahine, K. (2024). A comparative study of ensemble methods and multi-output classifiers for predictive maintenance of hydraulic systems. *Results in Engineering*, *24*, 102900. https://doi.org/10.1016/j.rineng.2024.102900
29. Olaniyi, R., Olugbile, H., & Okwuobi, O. (2025). The Role of Artificial Intelligence In Networking: A Review. *Gen-Multidisciplinary Journal of Sustainable Development*, *3*(1), 15-45. https://gmjsd.org/journal/index.php/gmjsd/article/view/75
30. Ouhssini, M., Karim Afdel, A. M., E. Agherrabi, & Abdallah Abarda. (2024). Advancements in detecting, preventing, and mitigating DDoS attacks in cloud environments: A comprehensive systematic review of state-of-the-art approaches. *Egyptian Informatics Journal*, *27*, 100517–100517. https://doi.org/10.1016/j.eij.2024.100517
31. Pandian, J. A., Kumar, V. D., Geman, O., Hnatiuc, M., Arif, M., & Kanchanadevi, K. (2022). Plant disease detection using a deep convolutional neural network. *Applied Sciences*, *12*(14), 6982. https://doi.org/10.3390/app12146982
32. Ragupathi, C., Dhanasekaran, S., Vijayalakshmi, N., & Salau, A. O. (2024). Prediction of electricity consumption using an innovative deep energy predictor model for enhanced accuracy and efficiency. *Energy Reports*, *12*, 5320–5337. https://doi.org/10.1016/j.egyr.2024.11.018
33. Shivaji, S. (2024). DDoS attack detection: Strategies, techniques, and future directions. *J. Electrical Systems*, *20*(9s), 2030-2046. https://www.researchgate.net/profile/Vinay-Patil-12/publication/382393041_DDoS_Attack_Detection_Strategies_Techniques_and_Future_Directions/links/669aac0802e9686cd1107e1e/DDoS-Attack-Detection-Strategies-Techniques-and-Future-Directions.pdf
34. Singh, A., & Gupta, B. B. (2022). Distributed Denial-of-Service (DDoS) Attacks and Defence Mechanisms in Various Web-enabled Computing Platforms. *International Journal on Semantic Web and Information Systems*, *18*(1). https://doi.org/10.4018/ijswis.297143
35. Sudaryono, S., Pratomo, R., Ramadan, A., Ahsanitaqwim, R., & Fletcher, E. (2025). Artificial Intelligence in Predictive Cybersecurity: Developing Adaptive Algorithms to Combat Emerging Threats. *Journal of Computer Science and Technology Application*, *2*(1), 1–13. https://doi.org/10.33050/xgt43743
36. Sudaryono, S., Pratomo, R., Ramadan, A., Ahsanitaqwim, R., & Fletcher, E. (2025). Artificial Intelligence in Predictive Cybersecurity: Developing Adaptive Algorithms to Combat Emerging Threats. *Journal of Computer Science and Technology Application*, *2*(1), 1–13. https://doi.org/10.33050/xgt43743
37. Veisi, H. (2023). Introduction to SVM. In *Learning with Fractional Orthogonal Kernel Classifiers in Support Vector Machines: Theory, Algorithms and Applications* (pp. 3-18). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-6553-1
38. Waqas, H., & Henry, T. (2025). *Machine Learning-Powered Intrusion Detection Systems for IoT and Cloud Environments.* https://www.researchgate.net/profile/Theodore-Henry-5/publication/389313763_Machine_Learning-Powered_Intrusion_Detection_Systems_for_IoT_and_Cloud_Environments/links/67bdcacb96e7fb48b9cd18f8/Machine-Learning-Powered-Intrusion-Detection-Systems-for-IoT-and-Cloud-Environments.pdf
39. Xiang, Q., Wu, S., Wu, D., Liu, Y., & Qin, Z. (2025). Research on CNN-BiLSTM Network Traffic Anomaly Detection Model Based on MindSpore. *arXiv preprint arXiv:2504.21008.* https://doi.org/10.48550/arXiv.2504.21008
40. Xu, S., Song, Y., & Hao, X. (2022). A comparative study of shallow machine learning models and deep learning models for landslide susceptibility assessment based on imbalanced data. *Forests*, *13*(11), 1908. https://doi.org/10.3390/f13111908
41. Zhang, Y., Liu, Y., Guo, X., Liu, Z., Zhang, X., & Liang, K. (2022). A BiLSTM-based DDoS attack detection method for edge computing. *Energies, 15*(21), 7882. https://doi.org/10.3390/en15217882
42. Zhou, H., & Ling, J. (2023). A Cooperative Detection of DDoS Attacks Based on CNN-BiLSTM in SDN. *International Journal of Future Computer and Communication, 12*(2), 27–36. https://doi.org/10.1088/1742-6596/2589/1/012001