
Hybridized Machine Learning based IDS for Anomaly Detection: A Systematic Review

Victor Mathebula¹, Bukohwo Michael Esiefarienrhe²

victorwaleriver@gmail.com¹, michael.esiefarienrhe@nwu.ac.za²

^{1,2} Department of Computer Science and Information Systems, North-West University, Mahikeng, South Africa

Article Information

Received : 26 Mar 2026

Revised : 10 May 2026

Accepted : 25 May 2026

Keywords

hybrid machine learning,
intrusion detection
system, anomaly
detection

Abstract

Intrusion Detection Systems play a crucial role in safeguarding networks against increasingly sophisticated cyber threats. Traditional Intrusion Detection Systems approaches often struggle with adaptability and high false-positive rates. This review investigates the use of hybridized Machine Learning models for anomaly detection in IDS to enhance detection accuracy and system robustness. This study applies the PRISMA framework to analyze hybrid machine learning techniques applied to improve the performance of Intrusion Detection Systems, the datasets used, performance evaluation, identification of challenges, and knowledge gap analysis. Results show that hybrid ML models consistently outperform single-model approaches, achieving an accuracy of up to 99.99%. Despite promising results, challenges such as class imbalance and limited real-time deployment persist. From this systematic review, it is evident that hybridizing machine learning algorithms in Intrusion Detection Systems offers a powerful approach to anomaly detection, improving precision and accuracy.

A. Introduction

Artificial Intelligence (AI) systems can search enormous amounts of data, identifying anomalies before initiating automated responses [1]. Machine Learning (ML) is a subfield of AI that uses computer science, statistics, and advanced mathematics to acquire knowledge from data [2]. Intrusion Detection Systems (IDS) are crucial software solutions designed to automate the monitoring and analysis of network intrusions, aiming to detect and prevent unauthorised access to systems [3]. These systems play a vital role in enhancing network security and safeguarding against the constantly evolving landscape of cyber threats [4]. As a secondary layer of defence following firewalls, IDSs ensure real-time security by monitoring network behaviour to identify and mitigate both external and internal attacks [5].

Intrusions are any attempts to compromise the confidentiality, integrity, or availability of a network or computer system, or to bypass its security mechanisms [4]. Given the rising frequency and sophistication of cyber-attacks across various sectors, network security has become a critical area of research requiring continuous advancements and improvements in IDSs to maintain data confidentiality and integrity [4]. As cyberattacks become increasingly sophisticated, there is a growing need for automated, intelligent systems that can detect and respond to threats in real-time. The integration of Artificial Intelligence (AI) or Machine Learning (ML) techniques into IDSs has shown promise in enhancing their capabilities [6]. A hybrid ML technique, which leverages the strength of supervised and unsupervised learning, can improve the precision and automation of anomaly detection, perform real-time evaluations, and adapt through self-learning from continuous data streams [7].

IDSs can be categorized based on their implementation and detection methods. The primary types of intrusion detection are anomaly-based and signature-based [3]. Anomaly-based IDSs monitor incoming traffic and raise alarms when deviations from normal behaviour exceed predefined thresholds [4]. However, this method often suffers from high false-positive rates [3].

This study aims to review the current state of AI/ML-based IDS research, focusing on the hybridized ML models for anomaly detection to prevent intrusions in computer networks. The review focuses on IDS that uses anomaly detection for intrusion detection, the methodologies presented in the research articles, the ML optimisation techniques presented, and the performance of the presented ML algorithms.

The rest of this paper is structured as follows: Section B provides the systematic literature review method. Section C discusses the results from the literature. The paper concludes in Section D by providing a summary of the work and future directions.

B. Research Method

A research method for this systematic literature review is conducted by applying the PRISMA framework to search and analyze research papers relevant to this study. A search strategy is formulated, followed by the inclusion criteria, exclusion criteria, and quality assessment.

1. Selection of research papers

For this literature review, a strategy was developed to identify relevant literature. The search strategy was to search for the following keywords: Intrusion Detection System, Artificial Intelligence, Hybrid Machine Learning model, and Anomaly Detection. These keywords were searched on Google Scholar, which led to the discovery of the intended databases, ScienceDirect and IEEE Xplore.

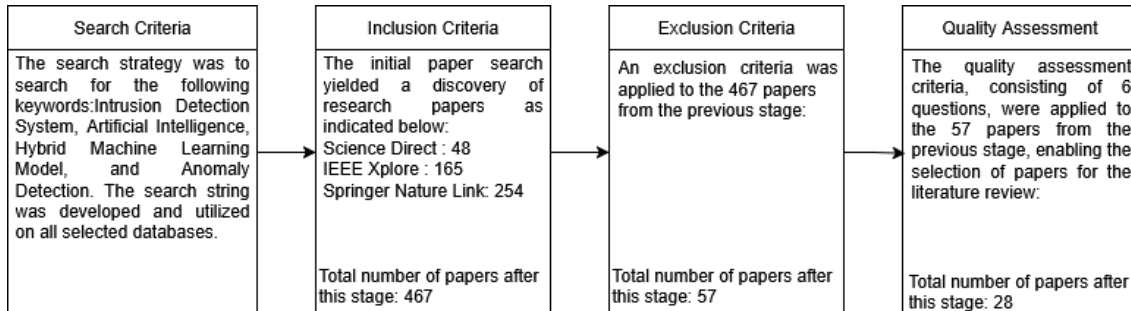


Figure 1. Selection of research papers

2. Formulating a research term

The keywords that appear on the research questions influenced the terms appearing on the search term. The keywords referred to are AI, ML, IDS, Hybrid and Anomaly Detection. All the identified keywords are essential in sourcing the relevant research papers. As such, the Boolean operator “AND” was chosen as the operator to link all the keywords in the search term.

The search term applied for this literature review is “Intrusion Detection System” AND “Artificial Intelligence” AND “Hybrid Machine Learning model” AND “Anomaly Detection”. The same search term was applied to ScienceDirect and SpringerLink. The search term was applied to IEEE Xplore without the use of a Boolean operator. The key terms were separated by commas. The following discipline and subdisciplines were specified on the SpringerLink, respectively, “Computer Science” and “Artificial Intelligence, Computer Communication Networks”, and “Computer Science, General” to limit the search results to the search term presented.

The databases utilized for this Systematic Literature Review are IEEE Xplore, Springer Nature Link, and ScienceDirect.

3. Inclusion Criteria

A total of 254 papers met the initial search criteria from Springerlink, ScienceDirect, and IEEE Explore combined. ScienceDirect identified 48 papers, followed by IEEE Xplore with 165. A total of 467 papers were selected for this review. The inclusion criteria for the selected papers are as follows:

Inclusion Criteria 1: The paper published is written in English.

Inclusion Criteria 2: The paper was published in 2021 or later.

Inclusion Criteria 3: Including published conference papers and journal papers,

Inclusion Criteria 4: The paper discusses hybrid ML techniques, models, or frameworks and rates their performance.

Inclusion Criteria 5: The paper applies an experimental or simulation approach in its methodology.

4. Exclusion Criteria

A criterion for excluding papers from the previous stage was initiated. The exclusion criteria on the available papers are as follows:

Exclusion criteria 1: Exclude case reports, editorials, reviews

Exclusion criteria 2: Exclude papers that only discuss IDS integration with AI without using ML and anomaly detection methods.

Exclusion criteria 3: Exclude papers that do not discuss hybrid ML algorithms, models, or frameworks.

Exclusion criteria 4: Exclude studies that are not relevant to the research questions

5. Quality Assessment

Quality assessment was performed according to the six questions listed in Table 1. Only research papers that satisfied most of the questions were selected.

Table 1. Quality assessment questions

No	Quality Assessment Question	Yes/No/Partially
1	Does the paper aim to enhance IDS using AI\ML algorithms?	
2	Does the paper present a hybrid ML model or framework?	
3	Does the ML model detect intrusions using the anomaly detection method?	
4	Are the ML techniques discussed that enhance the performance of the model?	
5	Is there a comparative analysis of the ML model presented with other models?	
6	Does the paper analyze the performance of the presented ML model and present the accuracy?	

6. Data extraction

Relevant data from each selected research paper was extracted to an external file. The fields of interest in this literature review are the database where the article is published, the authors of the paper, the title of the paper, the year in which it was published, the publication type (Journal, Conference paper, etc), the methodology used, the findings and results, and the recommendations from the authors. Table 2 shows each field and an example of each data parameter from one article.

Table 2. Data extraction method

Field	Data
Database	ScienceDirect
Authors	Edmund Fosu Agyemang
Title	Anomaly detection using unsupervised machine learning algorithms: A simulation study
Year	2024
Publication type	Conference
Methodology	Experimental

Findings and results	A hybrid of OC-SVM and SGD performed Better with an accuracy of 91.36%, precision of 100%, however, recall and F1 score were low at 5% and 9.52% respectively.
Recommendations and future work	The choice of the anomaly detection algorithm should depend on the characteristics of the dataset and the application requirements. Future work should investigate hybrid anomaly detection.

A total of 28 research papers were selected after the rigorous process of choosing the most relevant papers that address the hybrid ML model or frameworks. Of the 28 research papers, the majority came from IEEE Xplore, at 64%, followed by ScienceDirect at 22%, and SpringerLink contributed the least, with 14%. Regarding publication types, 54% of the research papers were published as conference papers, while 46% were journal papers.

In terms of the year of publication, most of the articles in this literature review were published in 2024. A total of eight research papers were published in 2024, followed by 2023 and 2025, with seven articles each. Three papers were published in 2021 and 2022 for each year. This analysis reveals an upward trend in the number of articles published annually on hybrid ML-based IDS.

Figures 2, 3, and 4 show the Article Databases, Publication Type, and Publication Years, respectively.

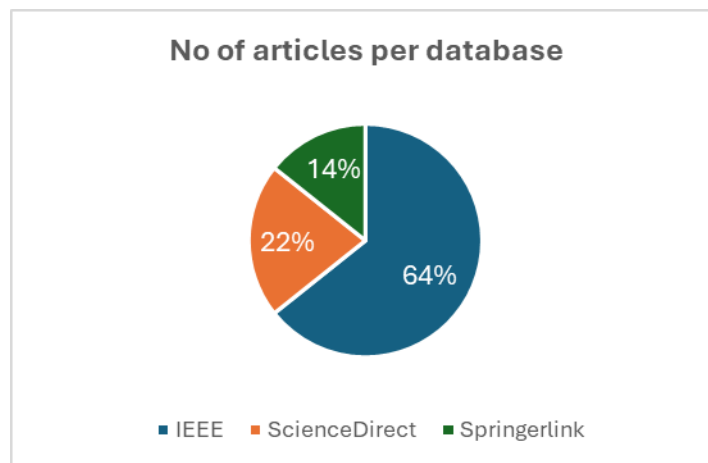


Figure 2 Database comparison

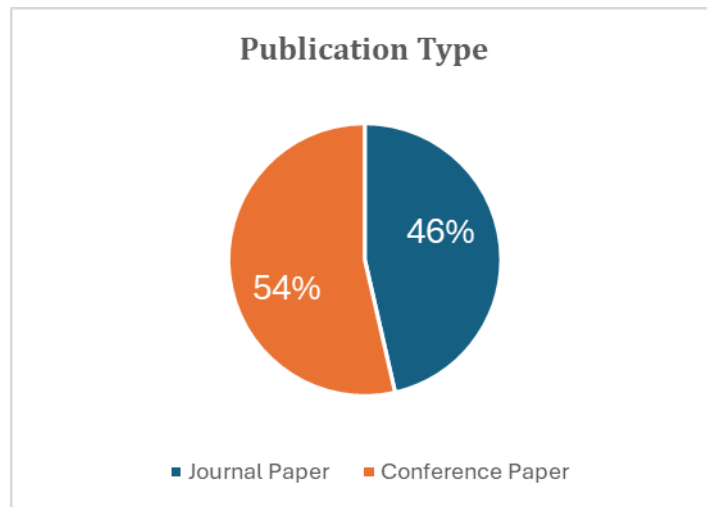


Figure 3. Article publication type

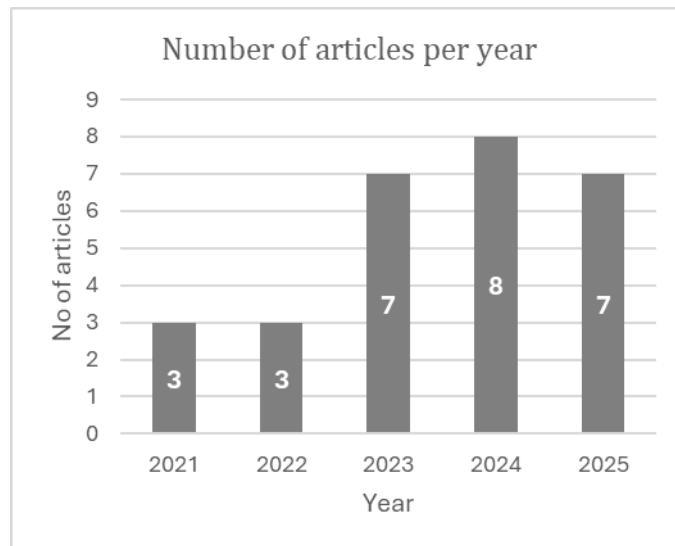


Figure 4 No of articles per year

7. Data Synthesis

Table 3 lists and compares all relevant articles visited for a literature review. This table indicates the presence of keywords or concepts related to the study, such as Intrusion Detection, AI, ML models or frameworks, Anomaly Detection, and ML model optimization techniques, as well as ML model evaluation, in each article associated with the literature review of this study. All articles addressed Intrusion Detection or Anomaly Detection using ML algorithms. ML and AI keywords were used interchangeably, but with a focus on the application of ML techniques or algorithms.

Table 3 Presence of key concepts (X = not mentioned, ✓ = covered, ○ = partially)

No	Author	<i>Intrusion Detection</i>	<i>Artificial Intelligence</i>	<i>Hybrid Machine Learning</i>	<i>Anomaly Detection</i>	<i>ML Model or Framework</i>	<i>Model or Framework Optimization</i>	<i>Model or Framework Evaluation</i>
1	[8]	X	✓	✓	✓	✓	✓	✓
2	[3]	✓	✓	✓	✓	✓	✓	✓
3	[9]	X	✓	✓	✓	✓	○	✓
4	[10]	✓	✓	✓	✓	✓	✓	✓
5	[11]	✓	✓	✓	✓	✓	✓	✓
6	[2]	X	✓	✓	X	✓	○	✓
7	[12]	✓	X	✓	✓	✓	○	✓
8	[13]	✓	✓	✓	✓	✓	○	✓
9	[14]	✓	✓	✓	✓	✓	○	✓
10	[15]	✓	X	✓	✓	✓	X	✓
11	[16]	X	✓	✓	✓	✓	✓	✓
12	[17]	✓	X	✓	✓	✓	✓	✓
13	[18]	✓	X	✓	✓	✓	○	✓
14	[19]	✓	X	✓	✓	✓	○	✓
15	[20]	✓	X	✓	✓	✓	✓	✓
16	[21]	✓	X	✓	✓	✓	✓	✓
17	[22]	✓	X	✓	✓	✓	✓	✓
18	[23]	✓	X	✓	✓	✓	✓	✓
19	[24]	✓	✓	✓	✓	✓	X	✓
20	[25]	✓	X	✓	✓	✓	○	✓
21	[26]	✓	✓	✓	✓	✓	○	✓
22	[27]	✓	✓	✓	✓	✓	○	✓
23	[28]	✓	✓	✓	✓	✓	✓	✓
24	[29]	✓	✓	✓	✓	✓	X	X
25	[30]	✓	✓	✓	✓	✓	○	✓
26	[31]	✓	✓	✓	✓	✓	X	✓
27	[32]	✓	✓	✓	✓	✓	✓	✓
28	[33]	X	✓	✓	✓	✓	✓	✓

C. Results and Discussion

ML algorithms have improved the functionality of IDS and its performance [19]. They have been successfully implemented in systems such as IoT to detect anomalies [26]. Supervised and unsupervised learning models are the most applied in ML models [10]. Unsupervised models reduce the necessity for data labelling because they can identify unknown threats without any prior knowledge, while supervised models learn from labelled data [3].

1. Hybrid Machine Learning methods

The hybrid approach combines several algorithms to improve detection accuracy by leveraging the advantages of various ML methods [24]. Several studies tried to improve IDS performance by integrating several ML models to formulate a hybrid model [18]. It has been demonstrated in various studies that hybrid models are a powerful, broadly applicable solution for the IDS; they outperform single model solutions in terms of accuracy and false positive reduction[24]. The two hybrid techniques (Stacking and Voting) are explained as follows: Stacking applies layers of ML models sequentially to achieve better detection and classification performance[24]. The voting method combines multiple predictions from various models, intending to improve overall performance [22].

2. Machine Learning algorithms and performance

We reviewed various proposed framework from the literature to determine the ML algorithm utilised and their performance. Various studies applied different ML algorithms aiming to achieve different objectives, particularly in IDS. ML algorithms such as SVM, KNN, RF, and DT are common and effective for anomaly detection [24].

Table 4 presents the author, the purpose of the article, ML algorithms applied, and the accuracy of the model. The accuracy of each model was determined by using parameters (True Positive, False Positive, False Negative and False Positive) from the Confusion Model. The accuracy is determined by the number of samples that are correctly classified from a complete dataset [26]. The performance of ML-based IDS can also be determined by measuring their Precision, Recall, F1-score, and ROC-AUC.

Models developed by Talukder et al.[28] and Usoh et al.[26] produced near-perfect accuracy of 99,99% each, showing their effectiveness in anomaly detection in IDS. Aygemang [33] produced the lowest performing model compared to other models in Table 4, with an accuracy of 91.36%. This shows the need for improvement and enhancement of various existing models in IDS.

Table 4 ML models and their performance

No	Author	Purpose	ML Algorithms	Accuracy %
1.	[11]	Enhancement of IDS effectiveness using ML	Random (RF)and SVM	Forest 98.98
2.	[2]	to create and assess ML models that would accurately detect and monitor phishing attacks.	Decision Tree (DT) and RF	96

3.	[12]	Novel approach to detect cyberattacks in the Industrial Internet of Things (IIoT).	KNN, ET, GB, AB, LDA, CART, linear regression (LR), Naïve Bayes (NB), and RF	99.8
4.	[13]	to present a more effective and accurate model for detecting anomalies	DBSCAN and Isolation Forest (IF)	98.9
5.	[14]	Developing an Intrusion detection system for a network interface device.	NB, K-Nearest Neighbors (KNN) and Support Vector Machines (SVM)	98.55
6.	[15]	Enhance the performance of IDS in VANET using ML	RF and Weighted k-means	96.93
7.	[17]	A hybrid approach aimed at improving IDS using feature selection and stacking ensemble.	MRF-BOR-LR	99.96
8.	[19]	A hybrid approach based on ML and DL to enhance IDS	Random Forest LSTM	97.8
	[20]	A hybrid model to detect day-zero attacks in a network	Autoencoders, Transformer-Based Detection, and IF	97.2
9.				
10.	[21]	A hybrid framework for enhancing binary classification	Random Forest Principal Component Analysis (PCA)	99.32
11.	[22]	A hybrid framework for DDoS detection in a network.	DT RF XGBoost LightGBM CatBoost Neural Network	96.64
12.	[23]	An ML-based IDS for the detection of new cyber threats in a cloud environment	SVM PCA	98.1
13.	[25]	A hard voting ML framework for cyber-attack detection in IIoT	RF, CatBoost, HGBC	99.85
14.	[26]	A ML-based IDS for the detection of cyber attacks IoT systems	LR, KNN, DT, RF, XGB, and ANN	99.99
15.	[27]	A ML-based IDS to enhance cybersecurity	RF, GBM, DNN	95.7
16.	[28]	A hybrid ML model for network intrusion detection	SMOTE + XGBoost RF	99.99
17.	[30]	A new technique for intrusion detection	LSTM CNN	97.8
18.	[31]	A hybrid detection method for a multi-model method	SVM VGG-11	97.6
19.	[32]	A dynamic IDS to detect intrusions in the critical information infrastructure	PCA Multi-Class SVM	97.64
20.	[33]	Anomaly detection model using unsupervised ML algorithms	One-Class SVM SGD	91.36

3. Dataset

Datasets are essential to cybersecurity research because they enable the identification, categorization, and prediction of abnormal activities [16]. Intrusion detection models are often validated by using a small number of publicly available datasets [17]. The dataset utilised for research is obtained unprocessed and

imbalanced [21]. ML model requires data to be transformed from its original form to a format that is structured for anomaly detection [20]. There are several preprocessing techniques that assist in feature selection, standardization, and noise reduction, which ultimately enhance the model's performance. Synthetic Minority Oversampling Technique (SMOTE) is popular in ML for balancing the class distribution to ensure the model is highly effective [34]. SMOTE achieves this by generating artificial samples for the minority class before processing [35].

This section explores various datasets utilised for modelling and testing of various ML algorithms for intrusion and anomaly detection. Table 5 presents a list of datasets and articles that utilized the dataset in their studies. The majority of studies in this literature review opted for the CICIDS2017 and CICIDS2018 datasets. These datasets were utilised by 12 studies combined. The NSL-KDD dataset was utilised by five studies. Some studies utilised multiple datasets in their study, such as Nalini et al.[13] and Huang et al.[17]. Datasets utilised in various studies are either private or publicly available.

Table 5 Datasets utilized

Dataset	Articles
Credit Card Dataset	[8]
CICIDS2017 and 2018	[13], [15], [16], [3], [11], [17], [18], [19], [20], [24], [25], [31]
Environmental Sensor Telemetry Data	[9]
NSL-KDD	[10], [13], [14], [24], [30]
Mendeley data repository (Phishing)	[2]
DS2OS	[12]
UNSW-NB15	[13], [17]
BoT-IoT	[26][18]
ToN IoT	[26]
open-source power dataset	[21]
KDDCUP'99	[28]
CIC-MalMem-2022	[28]
Private Dataset	[22],[33], [32], [23], [29]
National Software Reference Library	[27]

4. Challenges in Machine Learning based IDS

ML can be applied in IDS for various purposes in various ways. While ML enhances the efficiency and accuracy of IDS, its application faces multiple challenges, such as robustness, explainability, scalability, and evolving threats. Challenges experienced vary per model and application. IoT environments present unique challenges for IDS due to resource constraints and unreliable communication channels [24]. Devi et al. [29] discussed the challenges and limitations that may be observed in IDS when applied in financial systems, such as the difficulty in detecting new threats, the false negative and false positive rates, and the need for a larger amount of data. [18] highlighted the challenges of class imbalance in real-network traffic datasets, requiring robust test methods for proposed frameworks.

5. Knowledge gap analysis

Table 6 presents an analysis of recommendations in IDS using AI/ML from various articles. From the literature reviewed, supported by the summary of recommendations in Table 6, the future of IDS calls for more enhancement techniques, such as hybridization of ML models, to handle emerging cyber threats.

Table 6. Knowledge gap identified

Author	Recommended focus
[29]	The authors called for an integrated approach to intrusion detection that integrates methods from artificial intelligence, network security, computer science, and data analytics. enhance IDS accuracy and effectiveness, integrating IDS with other security frameworks, and create strategies for dealing with emerging technologies and new threats. The future work should involve the investigation of models' performance against emerging threats from the latest databases.
[25]	The authors recommended for inclusion of various dataset to their proposed model.
[20]	Exploration of the implementation of real-time IDS on a large-scale network to improve detection and efficiency. Focus on integrating reinforcement learning and federated learning for decentralized intrusion detection to improve model adaptation to evolving cyber threats.
[36]	Improvement of the model's ability to respond to potential threats and investigate the integration with the latest technologies

D. Conclusion

This Systematic Literature Review explored various hybrid ML models and frameworks based on anomaly detection to classify intrusions. When conducting this systematic literature review, the PRISMA framework was followed. The search method was developed. The search term was formulated, and it was applied to the databases identified. The databases are Science Direct, Springer Nature link and IEEE Xplore. Initially, 1305 articles were identified, which were reduced to 28. Inclusion and exclusion criteria were applied to select the most relevant articles for this study. Furthermore, a quality assessment was conducted to ensure that high-quality research papers were utilised for this study. The articles identified for this research were analysed according to the year they were published, the publication type, and their source or databases.

From the literature, it is evident that by leveraging AI, anomaly detection systems can adapt dynamically to evolving threats, enabling organizations to stay ahead of cyber threats and proactively mitigate risks. However, the effectiveness of ML-based IDS relies heavily on the quality of the dataset used for training, as well as the sophistication of the algorithms and models employed. There is a need to integrate a hybrid ML approach into IDS due to its capabilities, such as accuracy and automation, which improve IDS performance and detection rates.

E. Acknowledgment

We acknowledge the support given to the researchers by the Umalusi, South Africa and permission to use their network data for the simulation aspects of this research.

F. References

- [1] S. Akilandeswari, T. R. Soumya, S. Sumathi, M. Sushith, V. Brinda, and S. Rajan, "A Hybrid CNN-LSTM-PSO Framework for Enhanced Cybersecurity Threat Detection and Classification," in *Proceedings of the International Conference on Multi-Agent Systems for Collaborative Intelligence, ICMSCI 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 1956–1965. doi: 10.1109/ICMSCI62561.2025.10894126.
- [2] P. Maturure, A. Ali, and A. Gegov, "Hybrid Machine Learning Model for Phishing Detection," *International IEEE Conference proceedings, IS*, no. 2024, pp. 1–7, 2024, doi: 10.1109/IS61756.2024.10705257.
- [3] S. Bhadauria and T. Mohanty, "Hybrid Intrusion Detection System using an Unsupervised method for Anomaly-based Detection," *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, vol. 2021-Decem, pp. 1–6, 2021, doi: 10.1109/ANTS52808.2021.9936919.
- [4] F. Nabi and X. Zhou, "Enhancing intrusion detection systems through dimensionality reduction: A comparative study of machine learning techniques for cyber security," *Cyber Security and Applications*, vol. 2, no. January, 2024, doi: 10.1016/j.csa.2023.100033.
- [5] C. Lu, "Research on the technical application of artificial intelligence in network intrusion detection system," *Proceedings - 2022 International Conference on Electronics and Devices, Computational Science, ICEDCS 2022*, pp. 109–112, 2022, doi: 10.1109/ICEDCS57360.2022.00031.
- [6] Z. Sun, G. An, Y. Yang, and Y. Liu, "Optimized machine learning enabled intrusion detection 2 system for internet of medical things," *Franklin Open*, vol. 6, no. November 2023, p. 100056, 2024, doi: 10.1016/j.fraope.2023.100056.
- [7] B. P. Aniruddha Prabhu and N. R. Sunitha, "A Literature Review on Machine Learning Methods Used in Intrusion Detection System to Detect Cyber Attack," in *2024 International Conference on Cybernation and Computation, CYBERCOM 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 94–97. doi: 10.1109/CYBERCOM63683.2024.10803215.
- [8] K. Negi, G. P. Kumar, G. Raj, S. Sahana, and V. Jain, "Degree of Accuracy in Credit Card Fraud Detection Using Local Outlier Factor and Isolation Forest Algorithm," *Proceedings of the Confluence 2022 - 12th International Conference on Cloud Computing, Data Science and Engineering*, pp. 240–245, 2022, doi: 10.1109/Confluence52989.2022.9734123.
- [9] S. Potharaju, R. K. Tirandasu, S. N. Tambe, D. B. Jadhav, D. A. Kumar, and S. S. Amiripalli, "A two-step machine learning approach for predictive maintenance and anomaly detection in environmental sensor systems," *MethodsX*, vol. 14, no. January, 2025, doi: 10.1016/j.mex.2025.103181.
- [10] S. Agrawal, G. K. Gupta, P. K. Gopalakrishna, V. S. Balasubramaniam, L. Goel, and S. Mahadik, "Hybrid Machine Learning Models: Combining Strengths of Supervised and Unsupervised Learning Approaches," *Proceedings of International Conference on Contemporary Computing and Informatics, IC3I 2024*, vol. 7, pp. 1056–1061, 2024, doi: 10.1109/IC3I61595.2024.10829140.
- [11] V. Sharma and D. J. Shah, "A Novel Approach to Intrusion Detection Systems Using Hybrid Machine Learning Techniques," *2024 International Conference*

- on Artificial Intelligence and Quantum Computation-Based Sensor Applications, ICAIQSA 2024 - Proceedings*, no. M1, pp. 1–6, 2024, doi: 10.1109/ICAIQSA64000.2024.10882184.
- [12] T. P. Jayesh, K. Pandiaraj, A. Paul, R. R. Chandran, and P. P. Menon, "A Hybrid Machine Learning Approach to Anomaly Detection in Industrial IoT," *ACCESS 2023 - 2023 3rd International Conference on Advances in Computing, Communication, Embedded and Secure Systems*, pp. 32–36, 2023, doi: 10.1109/ACCESS57397.2023.10199711.
- [13] M. Nalini, B. Yamini, C. Ambhika, and R. Siva Subramanian, "Enhancing early attack detection: novel hybrid density-based isolation forest for improved anomaly detection," *International Journal of Machine Learning and Cybernetics*, no. 0123456789, 2024, doi: 10.1007/s13042-024-02460-5.
- [14] A. Singhal, A. Maan, D. Chaudhary, and D. Vishwakarma, "A Hybrid Machine Learning and Data Mining Based Approach to Network Intrusion Detection," in *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 312–318. doi: 10.1109/ICAIS50930.2021.9395918.
- [15] H. Bangui, M. Ge, and B. Buhnova, "A hybrid data-driven model for intrusion detection in VANET," in *Procedia Computer Science*, Elsevier B.V., 2021, pp. 516–523. doi: 10.1016/j.procs.2021.03.065.
- [16] A. M. Salman, B. T. Al-Nuaimi, A. A. Subhi, H. Alkattan, and R. H. C. Alfihl, "Enhancing Cybersecurity with Machine Learning: A Hybrid Approach for Anomaly Detection and Threat Prediction," *Mesopotamian Journal of CyberSecurity*, vol. 5, no. 1, pp. 202–215, Jan. 2025, doi: 10.58496/MJCS/2025/014.
- [17] Y. Huang, G. Chen, J. Gou, Z. Fan, and Y. Liao, "A hybrid feature selection and aggregation strategy-based stacking ensemble technique for network intrusion detection," *Applied Intelligence*, vol. 55, no. 1, Jan. 2025, doi: 10.1007/s10489-024-06015-7.
- [18] Y. Wang, S. Cao, J. Li, and X. Zhang, "A Unified Framework for Hybrid Network Intrusion Detection," *IEEE Transactions on Network and Service Management*, 2025, doi: 10.1109/TNSM.2025.3609854.
- [19] K. Abhinav and V. Kumar, "A Hybrid Intrusion Detection System Using Machine Learning and Deep," in *2025 3rd International Conference on Communication, Security, and Artificial Intelligence, ICCSAI 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 1–7. doi: 10.1109/ICCSAI64074.2025.11064178.
- [20] A. Anjum, P. R. Subramanian, R. Stalinbabu, D. Kothapeta, K. S. Sheela, and B. Jegajothi, "Detecting Zero-Day Attacks using Advanced Anomaly Detection in Network Traffic," in *Proceedings of 5th International Conference on Pervasive Computing and Social Networking, ICPCSN 2025*, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 1247–1253. doi: 10.1109/ICPCSN65854.2025.11034868.
- [21] S. Tufail, H. Iqbal, M. Tariq, and A. I. Sarwat, "A Hybrid Machine Learning-Based Framework for Data Injection Attack Detection in Smart Grids Using PCA and Stacked Autoencoders," *IEEE Access*, vol. 13, pp. 33783–33798, 2025, doi: 10.1109/ACCESS.2025.3543751.

- [22] K. S. Rawat, P. Matta, A. Kotiyal, S. Kukreti, and G. Dangwal, "An Early Detection Mechanism for Distributed Denial of Service (DDoS) Attack Using Machine Learning Techniques," in *2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Applications, ICAIQSA 2024 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICAIQSA64000.2024.10882189.
- [23] P. Sirenjeevi and V. Dhanakoti, "Enhancing Network Security using Hybrid Machine Learning Techniques," in *Proceedings - 3rd International Conference on Advances in Computing, Communication and Applied Informatics, ACCAI 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ACCAI61061.2024.10601791.
- [24] V. Reddy, R. Sunitha, M. Anusha, S. Chaitra, and A. P. Kumar, "Artificial Intelligence Based Intrusion Detection Systems," in *4th IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICMNWC63764.2024.10872055.
- [25] R. Golchha, A. Joshi, and G. P. Gupta, "Voting-based Ensemble Learning approach for Cyber Attacks Detection in Industrial Internet of Things," in *Procedia Computer Science*, Elsevier B.V., 2022, pp. 1752–1759. doi: 10.1016/j.procs.2023.01.153.
- [26] M. Usuh, P. Asuquo, S. Ozuomba, B. Stephen, and U. Inyang, "A hybrid machine learning model for detecting cybersecurity threats in IoT applications," *International Journal of Information Technology (Singapore)*, vol. 15, no. 6, pp. 3359–3370, Aug. 2023, doi: 10.1007/s41870-023-01367-8.
- [27] A. Kataria, "An ML-Based Intrusion Detection System Design and Evaluation for Enhanced Cybersecurity," in *2023 International Conference on Communication, Security and Artificial Intelligence, ICCSAI 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 1036–1040. doi: 10.1109/ICCSAI59793.2023.10421690.
- [28] M. A. Talukder *et al.*, "A dependable hybrid machine learning model for network intrusion detection," *Journal of Information Security and Applications*, vol. 72, Feb. 2023, doi: 10.1016/j.jisa.2022.103405.
- [29] V. A. Devi, E. Bhuvaneshwari, and R. K. Tummala, "Decentralized Hybrid Intrusion Detection System for Cyber Attack Identification using Machine Learning," in *2023 International Conference on Data Science, Agents and Artificial Intelligence, ICDSAAI 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICDSAAI59313.2023.10452439.
- [30] P. Selvarajan, R. Salman, S. Ahamed, and P. Jayasuriya, "Networks Intrusion Detection Using Optimized Hybrid Network," in *International Conference on Smart Computing and Application, ICSCA 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/ICSCA57840.2023.10087611.
- [31] F. Chen, "Research on anomal flow detection based on Multi-model," in *Proceedings - 2022 International Conference on Informatics, Networking and Computing, ICINC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 151–158. doi: 10.1109/ICINC58035.2022.00038.

- [32] Adejimi, Sodiya, Ojesanmi, Falana, and Tinubu, "A dynamic intrusion detection system for critical information infrastructure," *Sci. Afr.*, vol. 21, no. March, p. e01817, 2023, doi: 10.1016/j.sciaf.2023.e01817.
- [33] E. F. Agyemang, "Anomaly detection using unsupervised machine learning algorithms: A simulation study," *Sci. Afr.*, vol. 26, p. e02386, 2024, doi: 10.1016/j.sciaf.2024.e02386.
- [34] A. Gaurav, B. B. Gupta, P. Chaurasia, V. Arya, R. W. Attar, and K. T. Chui, "AI-Powered Intrusion Detection for Secure and Efficient SDN in Network Virtualization," in *IEEE International Conference on High Performance Switching and Routing, HPSR*, IEEE Computer Society, 2025. doi: 10.1109/HPSR64165.2025.11038896.
- [35] N. Srivastav and R. Singh, "An Optimized Machine Learning Based Network Intrusion Detection Systems for Identification of Low-Occurrence Attacks," *SN Comput. Sci.*, vol. 6, no. 7, Oct. 2025, doi: 10.1007/s42979-025-04336-z.
- [36] A. H. I. E. Tariq, M. B. I. E. Tariq, and S. Lu, "Hybrid AI-Driven Techniques for Enhancing ZeroDay Exploit Detection in Intrusion Detection System (IDS)," in *2024 3rd International Conference on Artificial Intelligence, Internet of Things and Cloud Computing Technology, AIoTC 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 156–160. doi: 10.1109/AIoTC63215.2024.10748333.