International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

A Review of AI-Driven Intrusion Detection Techniques in Modern Cybersecurity: Challenges and Future Direction

Vishakha Tomar[1], Dr.Shashikant Pandey[2]
[1]M.Tech Scholar, [2] Professor, CSE , VNS Group of Institutions, Bhopal, M.P., India

***Abstract*—The use of Intrusion Detection Systems (IDS) is essential to modern cybersecurity due to the growth of digital communications and networked systems. Most methods for implementing IDS have been developed using Artificial Intelligence (AI) methodologies. AI implementations have a distinct advantage over other implementations. Unfortunately, however, to date, no in-depth studies have been conducted to analyze AI implementations for understanding their current capability to solve ID challenges. The present work provides a broad overview of the Artificial Intelligence (AI) powered IDS, with particular focus on ML and DL implementation types. An assessment is made on the capability of supervised methodologies to detect attacks through classification and evaluates the effectiveness of using unsupervised methodologies to find anomalies in unlabeled data. Additionally, DL models, such as Convolutional Neural Networks (CNN's), Long Short-Term Memory (LSTM's) and Gated Recurrent Units (GRU's) will be reviewed, due to their ability to automatically identify characteristics and detect sophisticated attack patterns. The purpose of the review is to demonstrate the advantages of DL over traditional ML when utilizing large quantities of data with high dimensions, as well as exploring the challenges associated with false alarms, data reliance, and computational intensity. The need for lightweight models, better real-time detection, hybrid techniques, and more flexibility to changing cyber threats are just a few of the research issues and future goals that are outlined in the paper's conclusion. The frameworks of IDS studied are then analyzed in detail, and concluding remarks and prospects are mentioned.**

***Keywords*—Cybersecurity, Intrusion Detection Systems, NIDS, Artificial Intelligence, Machine Learning, Deep Learning, Neural Networks**

I. INTRODUCTION

The vast volume and variety of data have grown dramatically following the rise of telecommunications and communication technologies associated with the internet. Intrusion Detection Systems IDS) are critical for the integrity and safety of computer systems [1]. IDS have been developed by researchers, academics, and practitioners to help identify and mitigate threats on a computer network as efficiently as possible [2]. By examining the traffic on a network through an IDS, the network traffic can be compared against a normal, baseline level of activity. Therefore, any irregularities or abnormal conditions can be considered potential evidence of an intrusion.

When it comes to protecting computer networks, intrusion detection systems are becoming an essential component [3]. Their capacity to keep an eye on network activity and spot any questionable or malevolent behavior is crucial for safeguarding sensitive data and stopping illegal access [4]. Although anomaly management frameworks have been established to identify assaults, bigger datasets need the development of complicated rules, which may be expensive, time-consuming, and prone to errors. Nevertheless, the firewall method has not worked well in multi-cloud settings [5].

Several ML methods have been created to categorize different kinds of attacks and detect anomalies. A component of artificial intelligence, ML has the ability to learn characteristics and adjust to changing surroundings. For intrusion detection, statistical and ML techniques have shown to be quite effective. In Ref.[6], the author examined the impact of MLalgorithms on ID and uncovered the capabilities of different MLalgorithms. The DL idea is a sophisticated kind of ML algorithm that has been established in response to the growth of crucial data in the cloud. This technique uses a tiered approach to identify speech and audio processing applications [7].

DL has several advantages, one of which is autonomous Feature Learning, which trains the model on massive datasets by extracting features automatically. Algorithms outperform MLalgorithms in terms of performance [8]. An efficient DL method may also address the main problem with FP and zero-day attacks. This study gives a quick review of several AI-based cloud and NID techniques. It compares IDS based on ML, DL, and Ensemble-Learning and examines and categorizes various AI-based IDS. Additionally, it offers a taxonomical overview of all the IDS that rely on AI. Therefore, this survey focuses on analyzing and comparing various AI-driven intrusion detection approaches to identify efficient, scalable, and real-time solutions for modern cybersecurity challenges.

The following paper summarization are:

- This paper provides an in-depth analysis of identification methods powered by AI for the purpose of improving modern cybersecurity systems.
- It analyzes different learning approaches for both classification of network traffic and detection of anomalies in unlabelled data.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

- The research indicates that the use of advanced systems will allow for automatic feature extraction and the classification of intrusion attack patterns within the domain of computer network security.
- Lastly, the paper discusses the significant obstacles such as computing complexity and false alarms and expresses a desire to develop systems that can be scalable, adaptive, and real-time (IDS).

The structure for the rest of the paper is shown here. Section II is an overview of intrusion detection systems (IDS) with concepts and significance and their importance in cyber security. Section III includes a discussion of the various types of AI based intrusion detection techniques and how they can improve detection performance. In section IV you will find a thorough review of research that has been done along with the identification of currently existing gaps in the research and providing future direction for research. Finally, section V summarizes the most important aspects of the paper and presents the conclusions drawn from the study.

II. Overview Of Intrusion Detection

Intrusion Detection System (IDS) is the process of keeping an eye out for harmful activity on a computer system or network, including as unauthorized access, misuse, or modification of system resources. In order to stop further data loss or forfeiture, ID aims to detect such behavior in real-time or almost real-time and take the necessary action. IDS's goal is to monitor system and network activity for anomalous patterns that could indicate an impending attack. A variety of methods, with behavior-based detection, anomaly-based identification, and signature-based identification, may be used by these host-or network-based systems to detect potential dangers. After an IDS identifies a potential threat, it may send a signal to security people or other automated response mechanisms (such as firewalls) to help stop or lessen the impact of the assault. ID is a crucial component of an all-encompassing security plan and may help businesses quickly and effectively identify and address security concerns. ID is an important cybersecurity issue that can be resolved technologically [9]. The typical IDSarchitecture as shown in Figure 1 [10].

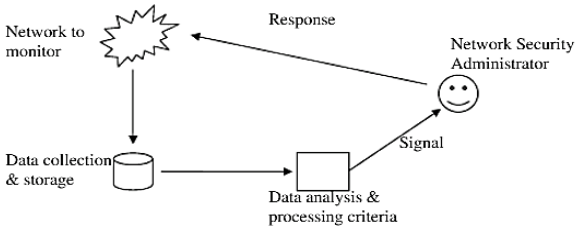

Fig. 1. Architecture of IDS[10]

A. *Types of IDS*

Despite the fact that all IDS serve the same objective, their methods of operation vary. There are several different kinds of IDS, including NIDS and HIDS, according to research [11]. Nonetheless, the two traditional IDS kinds that are most often used by businesses worldwide are:

1) *Network Intrusion Detection System (NIDS)*

The NIDS enables ID over whole network of the company, using all packet contents and metadata to identify threats. NIDS must be installed on hardware that is part of the organization's network infrastructure in order to utilize it. Once deployed, the NIDS will sample each packet that passes through it. NIDS are the most widely used form of IDS due to its ability to analyze all incoming and outgoing data, their ability to identify activities in real-time, which allows for faster reactions, their difficulty in being detected by intruders, and their strategic placement in key areas. However, manual maintenance and limited specificity are NIDS's key drawbacks [12].

2) *Host-Based Intrusion Detection System (HIDS)*

The HIDS monitors network traffic to and from a specified endpoint, keeps tabs on processes in execution, and examines system logs to and from a selected device. Despite having exhaustive insight into the host computer's internals, a HIDS can only see what's happening on its host system, limiting the decision-making environment. The HIDS's main benefits are its ability to be installed on computers or servers, its ability to identify the compromised device, its ability to notify administrators when analytical files are altered, and its particular efficacy against insider attacks. Regular monitoring is necessary for the appropriate use of HIDS [13].

B. *Methods of Intrusion Detection*

The IDS's purpose is to monitor network traffic after data collection and compare traffic patterns to identified attacks. Depending on the kind of IDS used by the enterprise, the security solution will rely on the following unique detection mechanisms to preserve the security of the network or information system:

1) *Signature-Based Intrusion Detection (SIDS)*

The goal of this detection approach is to find patterns, and then compare them to known evidence of intrusions. A database of previous invasions is essential to the SIDS technique (fig.1). The detection system will alert the network administrator if any network behavior fits the database's "signature" of an attack or breach [14]. Database revisions are frequently necessary because the SIDS is only capable of identifying assaults that are identifiable to it, and the database is the primary component of the SIDS.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

Nevertheless, this is regarded as the primary constraint of this approach, as the company will not be protected by any volume of database updates if it is the target of a new intrusion method.

2) Anomaly-Based Intrusion Detection (AIDS)

The ability of AIDS to detect this novel zero-day incursions is the main benefit of AIDS over SIDS, according to the literature. The AIDS technique builds "normal" behavior using ML and statistical data, and then the system will flag suspect traffic if it detects any deviation from this model. The potential for false positives, however, is said to be the biggest problem with AIDS compared to SIDS. The author contended that not all changes are the result of malevolent events, and that some are simply indicators of changes in the organization's behavior. Nevertheless, AIDS may interpret each anomaly as an intrusion, as it lacks a database of prior assaults for reference [15].

3) Hybrid Intrusion Detection

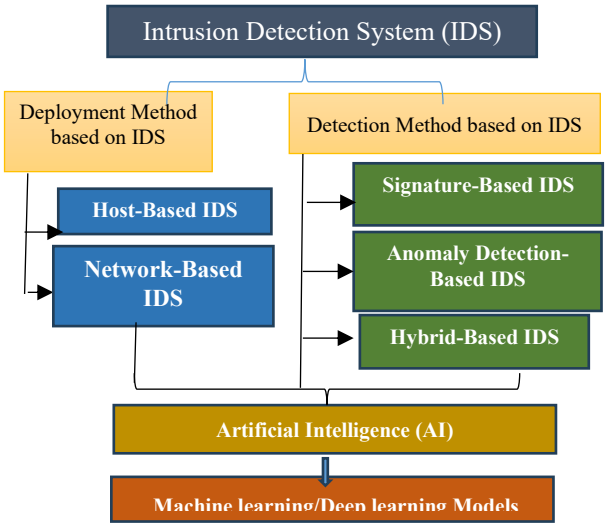

Fig. 2. Classification of IDSs [17]

The hybrid detection approach combines SIDS and AIDS. The hybrid system searches for patterns and one-time events to detect new and existing intrusion techniques. However, [16] emphasizes that this system is significantly constrained by an even greater increase in flagged issues. Nevertheless, it is challenging to perceive this increase in signals as a negative, given that the objective of IDS is to identify potential infringements[9].

Figure 2 illustrates an IDS classification that is determined by the detection approach and its environments. Consequently, it is necessary to implement suitable solutions to guarantee the cloud and network's functioning properly.

An appealing solution for the identification and classification of assaults is AI-based ID.

III. AI- Based Intrusion Detection Techniques

The term AI describes computer programs that can mimic human intellect in terms of learning, thinking, and decision-making. Even in the absence of direct human interaction, AI systems are up to evaluate vast amounts of data, spot patterns, and adjust to new data. Cybersecurity relies heavily on AI to improve real-time threat identification, prevention, and response. Traditional security systems depend on predetermined rules, in contrast to AI-based systems, which can learn fresh data and detect new, unknown assaults. The most popular AI techniques applied to complement IDS are ML, DL, and NN. These approaches enhance accuracy of threat detection and reduce false alarm and detection of suspicious activity. To sum up, AI allows IDS to improve their intelligence, adaptability, and efficiency in warding off cyberattacks. [1]

A. A general AI-based NIDS Methodology

Figure 3 illustrates three principal steps commonly followed in the creation of IDS based on use of ML and DL models: data preparation, training, and testing.

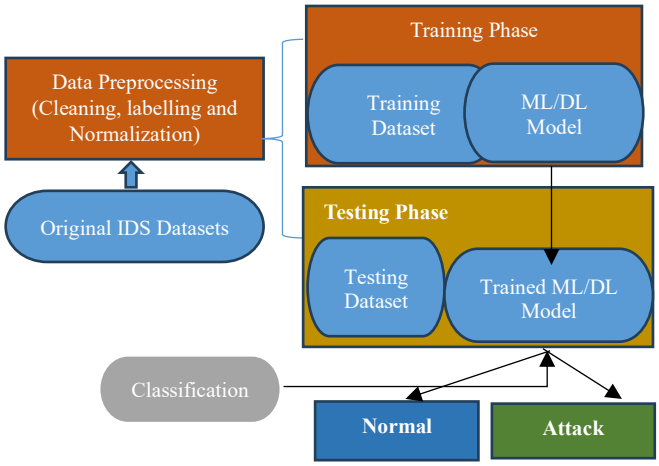

Fig. 3. General ML-DL-based IDS Flowchart [18]

The first step in implementing any of the suggested methods is to pre-process the dataset so that it can be used with the algorithm. Normalization and encoding are typically implemented during this phase. This step also involves the elimination of duplicate entries and those with missing data, which may entail dataset cleaning. The pre-processed data is divided into two datasets: train and test, which are generated at random. Nearly 80% of a dataset's initial size goes into training, while remaining 20% goes into testing.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

The training phase is ML or DL algorithm gets its hands on the training dataset. The dataset size and suggested model complexity dictate the learning duration of the method. Because of their complex structure, DL models may need longer training times than other model types. Next, the trained model is put to the test on the testing dataset and its performance is assessed by looking at its predictions. Network traffic examples are often labelled as benign (normal) or assault by IDS.

B. Machine Learning Techniques

The learning styles are taken into account while modelling the algorithm in AI, specifically in ML technologies. ML has been the most effective security technique for attack detection so far, and it seems like building an anomaly detection system requires a firm grasp of the system's semantic features [19]. Considerate threat model by classifying the behaviours of the attacker or the environment of the system is a prerequisite to building the ML-based security solution. The input data's characteristics make it the perfect option for the algorithm's categorization. Based on the available training data, ML primarily provides supervised and unsupervised methods for categorization. Figure 4 illustrates how both supervised and unsupervised learning are used in ML.

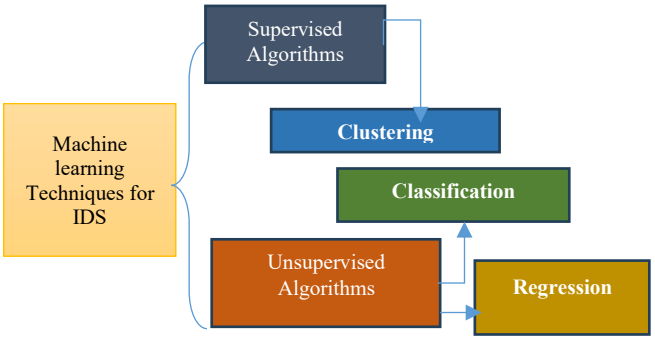

Fig. 4. ML methods include both unsupervised and supervised learning.

1) Supervised ML for Intrusion Detection

A ML assignment maps output data according to the relationships between input and output pairs. We have examined machine algorithms that are frequently employed in ID for empirical analysis. Based on train samples, primary aim of supervised learning style is to accomplish a specific objective. The most frequently encountered assignments in this learning approach are regression and classification mechanisms.

TABLE I.
SUPERVISED MACHINE LEARNING METHODS FOR INTRUSION DETECTION

Technique	Description	Advantages	Use in IDS
Support Vector Machine (SVM)[20]	A classification algorithm that separates data into classes using a hyperplane in high-dimensional space.	High accuracy in classification- Effective in high-dimensional data- Works well with clear margin separation	Classifies network traffic as normal or abnormal- Used with datasets like KDDCup99- Helps in feature selection and improving detection accuracy
Logistic Regression (LR)[21]	A probabilistic classification algorithm used for binary and multiclass classification based on sigmoid function.	Simple and efficient- Works well for linearly separable data- Provides probability outputs	Detects intrusions by predicting probability of attacks- Combined with feature selection methods like Genetic Algorithm- Applied on NSL-KDD dataset for attack classification
K-Nearest Neighbor (KNN)[22]	A non-parametric algorithm that classifies data based on similarity using distance metrics like Euclidean distance.	Easy to implement- No training phase required- Effective for pattern recognition	Classifies network traffic based on similarity to known data- Used with clustering methods for improved IDS performance- Applied in KDD datasets for attack detection
Bayesian (Naïve Bayes / Bayesian Networks) [23]	A probabilistic model based on Bayes' Theorem that predicts class probabilities using prior knowledge.	Fast and efficient- Works well with large datasets- Handles uncertainty effectively	Detects anomalous traffic using probability estimation- Used for feature selection and parameter estimation- Applied in IoT-based IDS and NSL-KDD dataset
Random Forest (RF)[24]	An EnsembleLearning technique that enhances classification accuracy by using numerous DT.	High accuracy and robustness- Reduces overfitting- Handles large datasets well	- Acts as a benchmark model in IDS- Detects complex attack patterns- Widely used in cloud and network security environments

2) Unsupervised ML for Intrusion Detection

This method makes advantage of similarity-based grouping. The hidden pattern in unlabelled database may be discovered by the model itself.

Using both clustering and association, the model may uncover the underlying dataset's hidden pattern. RealAI that replicates human learning abilities from prior experience is known as unsupervised learning

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

TABLE II.
UNSUPERVISED MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION

Technique	Description	Advantages	Use in Intrusion Detection Systems (IDS)
Fuzzy C-Means Clustering (FCM)[25]	A soft clustering method in that the distance from cluster centers determines the membership value of each data point, allowing it to belong to many clusters.	Handles overlapping data effectively- Provides flexible clustering- better stability and accuracy than hard clustering in some cases	Identifies and categorizes different types of network attacks- Used with KDD Cup 99dataset for training and testing- Helps detect anomalies based on likelihood scores- More effective than K-means in some intrusion detection scenarios
K-Means Clustering [26]	A clustering technique that uses centroid as its basis to divide data into K clusters, with every data point being assigned to group with the nearest centroid.	Simple and fast- Scalable to large datasets- Easy to implement	Used to detect anomalous network behavior- Acts as a preprocessing step before classification (e.g., with KNN, Naïve Bayes, 1R)- Helps group similar traffic patterns for attack detection- Applied on NSL-KDD and KDD Cup 99datasets

C. *Deep Learning Techniques*

DL may be seen of as a sophisticated progression of ML techniques and is a subset of ML. Layered structures are used by DL architectures to represent intricate ideas. The human brain serves as an inspiration for ANN, which in turn informs the design of DL structures. The DL technique is being used in a variety of disciplines, including Attack-Detection, and Image-Processing. DL models vary from ML models in terms of feature extraction. The program will learn from mistakes and automatically extract features using DL (Figure 4). DL need a large dataset in order to generate high-quality interpretations. These are thus superior than ML. Beyond that, DL discovers increasingly intricate connections and mappings between the two sets of data. This a subfield of ML that uses mathematical computing to learn via a network of interconnected layers called neurons [27].

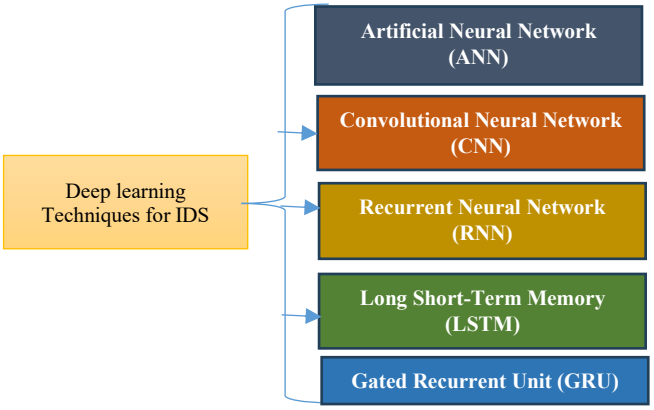

Fig. 5. Deep learning Methods for IDS

TABLE III.
DEEP LEARNING METHODS FOR INTRUSION DETECTION

Technique	Description	Advantages	Limitations	Use in IDS
Artificial Neural Network (ANN) [28]	A multi-layered neural network inspired by the human brain, where outputs from one layer are passed to the next for classification.	Good for classification tasks Learns complex patterns Flexible structure	Needs feature engineering- Prone to overfitting- Computational cost	Detects and classifies intrusions- Applied on KDD Cup 99 dataset- Evaluated using false positive/negative rates
Convolutional Neural Network (CNN) [29]	A DL model that automatically extracts spatial features using convolutional layers.	Automatic feature extraction- High accuracy Effective for large datasets	Requires large data- High computational complexity	Detects normal vs abnormal traffic- Achieves high accuracy (~97%)- Used with KDD and NSL-KDD datasets
Recurrent Neural Network (RNN) [30]	A sequential model that uses previous outputs as inputs, enabling memory of past data.	Captures temporal patterns Suitable for sequential data	Vanishing gradient problem- Slow training	Detects time-based attack patterns- Applied on UNSW-NB15 dataset
Long Short-Term Memory (LSTM) [31]	An advanced RNN variant that uses memory cells and gates to store long-term dependencies.	Solves vanishing gradient problem- Learns long-term dependencies- High accuracy in sequential data	High computational cost Complex architecture	Widely utilized for ID in sequential network traffic- Detects long-duration and stealth attacks- Improves accuracy over standard RNN
Gated Recurrent Unit (GRU) [32]	A simplified version of LSTM with fewer gates, designed to reduce complexity while maintaining performance.	Faster training than LSTM- Requires fewer parameters- Good performance on smaller datasets	Slightly less expressive than LSTM	Efficient for real-time IDS- Used in lightweight IDS systems- Balances accuracy and speed

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

IV. Literature Review

An IDS capability have been greatly improved by recent developments in AI and ML. Network intrusion detection has been the subject of several studies focusing on its security features in recent years. Table 5 provides a summary of the findings from the current surveys. An overview of key studies that explain present and future problems with AI-driven cybersecurity is given in this section.

Respecting the chronological release of each survey, the first current research by Z. Sun et al. (2023), research proposes an IDS for state-of-the-art health app platforms that detects and classifies malware data using a mix of PSO and AdaBoost algorithms. This research makes use of the NSL KDD dataset. There are 125,973 occurrences and 41 characteristics in the dataset, with testing comprising 80% and training 20%. Feature-Selection procedure employing PSO yields 12 important characteristics for intrusion detection. The IDS accurately classifies numerous attack, AdaBoost has the best rec value (0.966667) in terms of classifier performance, demonstrating its potent intrusion detection capabilities [33]. In this context, M. Chen et al. (2023) suggest the RCALN uncovering model that uses an alternating CNN-LSTM to extract traffic characteristics and incorporates Channel-Attention into CNNs. To further enhance the CNN-LSTM hybrid network, we also use residual networks to provide depth to the network's layers. Using three publicly available ID datasets, our model shows encouraging results [34].

In response to this issue, F. Guo et al. (2024), this article utilizes a method for detecting network intrusions that is based on ML. When building models, the ID module may make use of several techniques such as DL, SVM, etc. From 08:00 to 09:00, the real-time performance test results show an acc of 0.92. This article studies a machine learning based method for detecting and identifying network attack behaviours, which is beneficial for improving the level of network security defines [35].

To solve the issues of insufficient attack samples and low detection acc in NID, Y. Wei et al. (2024) this paper proposes a deep confidence NID method G-DBN based on GAN. The model is based on the malicious sample extension of the generative adversarial network, and it can produce adversarial samples using malicious network flows as original samples.

Furthermore, this paper uses deep belief network technology to create and assess an efficacy of the G-DB model in detecting network attacks, comparing it to standard DBN models and other network intrusion detection techniques. Experimental results show that compared to the standard three-layer DBN method, the G-DBN method described in this paper improves the detection accuracy of attack samples by 6.46% and better meets the performance requirements of current practical applications [36].

In the model training H. Liu et al. (2025), the CNN is adopted, and the parameters are updated by Adam optimization algorithm to enhance the model performance. The experimental evaluation uses KDD CUP 99 data set. The experimental outcomes show that CNNmodel has higher acc (92.3 %), rec (89.4 %) and F1score (90.5 %), in intrusion detection tasks, which is superior to traditional algorithms [37].

This article Z. Zhao (2025), explores the development and deployment of an AI-powered network IDS with the goal of enhancing detection accuracy and real-time efficiency. The adaptive learning and training procedure is then optimized using a One-Class SVM. An experimental outcome show that compared to the baseline systems of convolutional RNN and new DNN, the average accuracy of the system in this article is 4.7% and 6.5% higher, respectively, and the average response time decreases by 2.5 seconds and 4.1 seconds, respectively. The results indicate that AI-driven network IDS can provide more effective solutions for network security [38]. This study H. -W. Jeong et al. (2025), addresses the Class-Imbalance problem typically seen in network traffic data sets by presenting an LSTM-based NID model that integrates GAN-based oversampling. Investigating GAN-based oversampling for ID via comparative studies with various techniques, such as SMOTE and One-Class SVM, reveals both its benefits and drawbacks [39].

This study M. P. Venkatesh et al. (2026), presents a ML-based NIDS designed. The proposed system evaluates multiple classification algorithms, including RF, AdaBoost, XGBoost, and LR, for identifying abnormal network traffic patterns. Real-time testing shows an acc of 0.92 with a FAR of 0.05 between 08:00-09:00, and an acc of 0.90 with a FAR of 0.06 between 09:00-10:00. The average detection latency remained below 55 Ms across all intervals. Keywords-network intrusion detection, machine learning, real-time monitoring, anomaly detection[40]

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 03, March 2026)

TABLE IV.
RELATED WORK ON AI-DRIVEN INTRUSION DETECTION SYSTEMS

Ref	Author(s) & Year	Method / Model	Dataset Used	Key Features / Techniques	Performance Highlights	Limitations
[1]	Z. Sun et al. (2023)	PSO + AdaBoost	NSL-KDD	Feature selection using PSO (12 features), ensemble learning	Recall: 0.9667, high accuracy & precision	Limited to static dataset, lacks real-time validation
[2]	M. Chen et al. (2023)	RCALN (CNN + LSTM + Attention + ResNet)	Multiple public datasets	Channel attention, residual learning, hybrid deep learning	Strong feature extraction, improved detection accuracy	High computational complexity
[3]	F. Guo et al. (2024)	ML-based IDS (SVM, DL)	Not specified	Real-time detection, multiple ML models	Accuracy: 0.90–0.92, FAR: 0.05–0.06, latency: 50–55 ms	Limited dataset transparency
[4]	Y. Wei et al. (2024)	GAN + DBN (G-DBN)	Not specified	GAN-based data augmentation, deep belief networks	+6.46% accuracy improvement over DBN	Training complexity, GAN instability
[5]	H. Liu et al. (2025)	CNN + Adam Optimizer	KDD Cup 99	Data preprocessing, feature selection, deep CNN	Accuracy: 92.3%, Recall: 89.4%, F1: 90.5%	Uses outdated dataset
[6]	Z. Zhao (2025)	One-Class SVM (AI-driven IDS)	Not specified	One-hot encoding, sliding window, real-time detection	Accuracy improved by 4.7–6.5%, reduced response time	Limited comparison with modern DL models
[7]	H.-W. Jeong et al. (2025)	LSTM + GAN Oversampling	Not specified	GAN for class imbalance, sequence modeling	Improved anomaly detection vs SMOTE & SVM	GAN overhead, complexity
[8]	M. P. Venkatesh et al. (2026)	ML-based NIDS (RF, AdaBoost, XGBoost, LR)	Not specified	Multi-classifier evaluation, real-time monitoring	Accuracy: up to 0.92, latency <55 ms	Limited deep learning exploration

Research Gaps / Challenges: Despite major developments in AI-driven IDSs, numerous issues still exist:

- *Dataset Limitations and Realism:* Many studies use out-of-date benchmark datasets that do not correctly reflect contemporary network traffic, limiting the models' usefulness in real-world circumstances.
- *Class Imbalance and Data Scarcity:* Although data augmentation techniques are used, generating high-quality and representative synthetic data remains a challenge and can affect detection performance.
- *High Computational Complexity:* The advanced DL and hybrid models have high computing resource demands, that problematic to deploy them in real-time or in resource-constrained scenarios.
- *Limited Implementation in the Real-Time Environment:* While various performance metrics for each of various models were reported, nearly all of models have not been assessed in the real world, therefore, practical implementation issues such as scalability and flexibility have not been evaluated.
- *Inability to Generalize:* The majority of intrusion detection systems produce models that are primarily based on datasets used for training; therefore, models can be poorly generalized to different types of network conditions (both current and future), and have extreme difficulty dealing with new types of cyber threats (e.g., Zero Day Attacks).

A. Future Work/Direction

In the future, AI-based IDS research should look to develop:

- *Advanced Feature Selection:* Future research aiming to develop hybrid approaches that combine RFE with additional optimization techniques may lead to a greater number of relevant features and better model performance.
- *Improved Data Balancing Techniques:* Development of advanced synthetic sample generation techniques that allow for an accurate representation of the real world and balanced data samples. For example, SMOTE/GAN based data augmentation techniques are significantly better than random oversampling techniques currently used to balance datasets.

- *Ensemble and Hybrid Model Enhancement:* The RF and DT models can also be enhanced by combining them with other classifiers (XGBoost, SVM), which provides more accurate generalizations and stronger robustness through either ensemble or stacking methods.

Nevertheless, it can still be enhanced through the implementation of more advanced models, real-time testing, and more diverse data to make the system more flexible and responsive to real-life cybersecurity settings.

V. Conclusion

This paper has provided a comprehensive overview of current AI-based ID systems within the modern of computer security, including how the smart systems of today will continue to play an increasingly important role in securing network environments. Methods of ID (classification methods and anomaly detection methods) have been reviewed and found effective in identifying both well-known and unusual attack signatures. Advanced intelligent models are capable of identifying the appropriate features and automatically learning complex relationships from large and high dimensional datasets to improve detection accuracy and system performance. Also noted were limitations associated with these types of models; limitations that include, but are not limited to: high computational costs, the need to generate very large training corpus, and both False Positive and False Negative ratio issues that may impact on reliability. In addition, as the nature of cyber threats is constantly changing, so too must detection systems, therefore ongoing enhancement and adaptation be necessary. For this reason, it is critical that technologies that support real-time detection must be developed with an eye toward efficiency, light weight and scalability in future studies. In addition, combining hybrid solutions and improving model flexibility will be essential to creating resilient and trustworthy IDS that will be able to respond to the new cybersecurity challenges.

REFERENCES

[1] S. T and M. A. E.A, "A comprehensive review of AI based intrusion detection system," *Meas. Sensors*, vol. 28, p. 100827, Aug. 2023, doi: 10.1016/j.measen.2023.100827.

[2] M. K. Shah, "AI-Based Framework for Ransomware Detection in Android Systems: Enhancing Mobile Security," in *2025 5th International Conference on Artificial Intelligence and Signal Processing (AISP)*, IEEE, Nov. 2025, pp. 1–8. doi: 10.1109/AISP68263.2025.11396254.

[3] B. Madupati, M. M. Mohammed, L. Upadhyay, D. P. Guda, K. Kaushik, and M. Soni, "Integrating Artificial Intelligence with Cybersecurity for Resilient Wireless Communication Against Advanced Threats," in *2025 International Conference on Artificial Intelligence and Machine Vision (AIMV)*, IEEE, Aug. 2025, pp. 1–5. doi: 10.1109/AIMV66517.2025.11203666.

[4] V. Sharma, D. Shah, S. Sharma, and S. Gautam, "Artificial Intelligence based Intrusion Detection System A Detailed Survey," *ITM Web Conf.*, vol. 65, p. 04002, Jul. 2024, doi: 10.1051/itmconf/20246504002.

[5] S. Kumara, "A Lightweight Deep Learning Based Classification Models for Non-Human Identity Threat Detection," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395886.

[6] A. Binbusayyis, H. Alaskar, T. Vaiyapuri, and M. Dinesh, "An investigation and comparison of machine learning approaches for intrusion detection in IoMT network," *J. Supercomput.*, 2022, doi: 10.1007/s11227-022-04568-3.

[7] H. Cyril and S. Kumara, "Cybersecurity Architecture For Autonomous Telecommunication Networks," *Int. J. Adv. SIGNAL IMAGE Sci.*, vol. 12, no. 1s, pp. 618–639, Jan. 2026, doi: 10.29284/9admy374.

[8] R. V. S. S. B. R, Y. M. M. John, M. B. B. G, B. Karim, and G. Saritha, "Multi-Domain Cyber Threat Classification Using Enhanced Genetic Algorithm and Deep Neural Networks," in *2025 Third International Conference on Networks, Multimedia and Information Technology (NMITCON)*, IEEE, Aug. 2025, pp. 1–6. doi: 10.1109/NMITCON65824.2025.11187556.

[9] S. Muneer, U. Farooq, A. Athar, M. Ahsan Raza, T. M. Ghazal, and S. Sakib, "A Critical Review of Artificial Intelligence Based Approaches in Intrusion Detection: A Comprehensive Analysis," *J. Eng.*, vol. 2024, no. 1, Jan. 2024, doi: 10.1155/2024/3909173.

[10] G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: a review," *Artif. Intell. Rev.*, vol. 34, no. 4, pp. 369–387, Dec. 2010, doi: 10.1007/s10462-010-9179-5.

[11] L. H. Yeo, X. Che, and S. Lakkaraju, "Understanding Modern Intrusion Detection Systems: A Survey," *arXiv Comput. Sci.*, Nov. 2017.

[12] S. Ennaji, F. de Gaspari, D. Hitaj, A. Kbidi, and L. Vincenzo Mancini, "Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects," *IEEE Access*, vol. 13, pp. 148613–148645, 2025, doi: 10.1109/ACCESS.2025.3600984.

[13] Y. Shin and K. Kim, "Comparison of Anomaly Detection Accuracy of Host-based Intrusion Detection Systems based on Different Machine Learning Algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 2, 2020, doi: 10.14569/IJACSA.2020.0110233.

[14] M. Ahmed, A. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, Jan. 2016, doi: 10.1016/j.jnca.2015.11.016.

[15] A. N. Cahyo, A. Kartika Sari, and M. Riasetiawan, "Comparison of Hybrid Intrusion Detection System," in *2020 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, IEEE, Oct. 2020, pp. 92–97. doi: 10.1109/ICITEE49829.2020.9271727.

[16] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3041951.

[17] A. H. Ali *et al.*, "Unveiling machine learning strategies and considerations in intrusion detection systems: a comprehensive survey," *Front. Comput. Sci.*, vol. 6, Jun. 2024, doi: 10.3389/fcomp.2024.1387354.

[18] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, Jan. 2021, doi: 10.1002/ett.4150.

[19] M. Thakur, A. Jain, S. Khan, and D. P. Sen, "AI-Based Intrusion Detection Systems for Network Security: A Review," *Int. J. Sci. Manag. Eng. Res.*, 2025.

[20] P. Tao, Z. Sun, and Z. Sun, "An Improved Intrusion Detection Algorithm Based on GA and SVM," *IEEE Access*, vol. 6, pp. 13624–13631, 2018, doi: 10.1109/ACCESS.2018.2810198.

[21] E. Besharati, M. Naderan, and E. Namjoo, "LR-HIDS: logistic regression host-based intrusion detection system for cloud environments," *J. Ambient Intell. Humaniz. Comput.*, vol. 10, no. 9, pp. 3669–3692, Sep. 2019, doi: 10.1007/s12652-018-1093-8.

[22] A. D. Afifaturahman and F. MSN, "Perbandingan Algoritma K-Nearest Neighbour (KNN) dan Naive Bayes pada Intrusion Detection System (IDS)," *Innov. Res. Informatics*, vol. 3, no. 1, Mar. 2021, doi: 10.37058/innovatics.v3i1.2852.

[23] M. Panda, A. Abraham, S. Das, and M. R. Patra, "Network intrusion detection system: A machine learning approach," *Intell. Decis. Technol.*, 2011, doi: 10.3233/IDT-2011-0117.

[24] N. Zhu, C. Zhu, L. Zhou, Y. Zhu, and X. Zhang, "Optimization of the Random Forest Hyperparameters for Power Industrial Control Systems Intrusion Detection Using an Improved Grid Search Algorithm," *Appl. Sci.*, vol. 12, no. 20, p. 10456, Oct. 2022, doi: 10.3390/app122010456.

[25] T.-L. Nguyen, H. Kao, T.-T. Nguyen, M.-F. Horng, and C.-S. Shieh, "Unknown DDoS Attack Detection with Fuzzy C-Means Clustering and Spatial Location Constraint Prototype Loss," *Comput. Mater. Contin.*, vol. 78, no. 2, pp. 2181–2205, 2024, doi: 10.32604/cmc.2024.047387.

[26] S. Karim, M. Rousanuzzaman, P. A. Yunus, P. H. Khan, and M. Asif, "Implementation of K-Means Clustering for Intrusion Detection," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2019, doi: 10.32628/cseit1952332.

[27] M. K. Pasupuleti, "AI-Based Intrusion Detection Systems Using Ensemble Deep Learning Models," *Int. J. Acad. Ind. Res. Innov.*, vol. 05, no. 06, pp. 372–385, Jun. 2025, doi: 10.62311/nesx/rphcrcscrcp1.

[28] P. S. Aswale, D. P. Patil, and O. S. Vaidya, "Securing Cyber Physical System Using Machine Learning: A Survey on Attack Resistant Algorithms," *Rev. d'Intelligence Artif.*, vol. 38, no. 1, pp. 277–284, 2024, doi: 10.18280/ria.380129.

[29] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Survey of CNN-Based Network Intrusion Detection," *Appl. Sci.*, vol. 12, no. 16, p. 8162, Aug. 2022, doi: 10.3390/app12168162.

[30] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[31] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," *Sci. Rep.*, vol. 15, no. 1, p. 1554, Jan. 2025, doi: 10.1038/s41598-025-85248-z.

[32] Z. Wang, H. Huang, R. Du, X. Li, and G. Yuan, "IoT Intrusion Detection Model based on CNN-GRU," *Front. Comput. Intell. Syst.*, vol. 4, no. 2, pp. 90–95, Jun. 2023, doi: 10.54097/fcis.v4i2.10302.

[33] 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, p. 100056, Mar. 2024, doi: 10.1016/j.fraope.2023.100056.

[34] M. Chen, X. Luo, Y. Zhang, Z. Duan, and F. Li, "RCALN: A Hybrid Intrusion Detection System Incorporating Channel Attention in CNN and Residual Networks with LSTM," in *Proceedings - 2023 International Conference on Computer Science and Automation Technology, CSAT 2023*, 2023. doi: 10.1109/CSAT61646.2023.00125.

[35] F. Guo, H. Jiao, X. Zhang, Y. Zhou, and H. Feng, "Information Security Network Intrusion Detection System Based on Machine Learning," in *2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024*, 2024. doi: 10.1109/ICDSNS62112.2024.10691041.

[36] Y. Wei *et al.*, "A Deep Belief Networks Intrusion Detection Method Based on Generative Adversarial Networks," in *2024 5th International Seminar on Artificial Intelligence, Networking and Information Technology, AINIT 2024*, 2024. doi: 10.1109/AINIT61980.2024.10581576.

[37] H. Liu, S. Li, D. Li, Z. Wang, and D. Lun, "Design of Artificial Intelligence Aided Network Intrusion Detection System for Critical Infrastructure," in *Proceedings - 2025 International Conference on Digital Analysis and Processing, Intelligent Computation, DAPIC 2025*, 2025. doi: 10.1109/DAPIC66097.2025.00172.

[38] Z. Zhao, "Design and Implementation of Artificial Intelligence-Driven Network Intrusion Detection System," in *International Conference on Intelligent Systems and Computational Networks, ICISCN 2025*, 2025. doi: 10.1109/ICISCN64258.2025.10934308.

[39] H.-W. Jeong, H.-G. Kim, and Y.-H. Choi, "LSTM-Based Network Intrusion Detection System and Solving Data Imbalance Problem Through GAN," in *2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, IEEE, Feb. 2025, pp. 1156–1159. doi: 10.1109/ICAIIC64266.2025.10920641.

[40] M. P. Venkatesh, N. K. V, S. Saraswathi, and K. Abinaya, "AI Powered Network Intrusion Detection System Using Machine Learning," in *2026 5th International Conference on Communication, Computing and Electronics Systems (ICCCES)*, IEEE, Jan. 2026, pp. 195–200. doi: 10.1109/ICCCES62661.2026.11436357.