Journal of Global Research in Electronics and Communication
Volume 2, No. 5, May 2026
Available Online at: www.jgrec.info
RESEARCH PAPER

Advancing Cybersecurity with AI for Intrusion Detection Systems: A Review and Analysis of Tools, Techniques, and Challenges

Girish Thakre
M.Tech scholar
CSE Tit Excellence
Bhopal, India
girishthakre2002@gmail.com

Manish kumar Rohila
Assistant Professor
CSE Tit Excellence
Bhopal India
manishvds2004@gmail.com

Arjun Rajput
Assistant Professor
CSE Tit Excellence
Bhopal India
rajaarjun07@gmail.com

Saurabh Karsoliya
Technocrats Institute of Technology,
Bhopal, India
karsoliya.saurabh@gmail.com

***Abstract*—The state of cybersecurity can be improved with the help of AI-based Intrusion Detection Systems (IDS) because they enable the recognition of sophisticated threats in a dynamic network environment in an intelligent, dynamic, and real-time manner. The paper goes even deeper into the design of IDS, such as host-based, network-based, and hybrid, followed by the conventional detection methods, such as signature-based, anomaly-based, and specification-based. The paper continues to discuss the more advanced AI practices, noting ML and DL models such as SVM, Random Forest, CNN, and LSTM, which enhance the identification of known and zero-day attacks. The report continues by examining some of the enabling technologies, such as cloud-based IDS, Big data streaming platforms such as Kafka and Spark, AI-based security applications, and ML frameworks. Applications, such as real-time monitoring, multi-tenant security and DevSecOps integration, are explained alongside problematic issues, which are noisy data, computational overhead, encrypted traffic, adversarial attacks and limited real-world implementation. Overall, this study emphasises the need for AI-based IDS that are scalable, efficient, and strong enough to tackle all the new cyber threats.**

***Keywords*—Artificial Intelligence (AI), Intrusion Detection Systems (IDS), Cybersecurity Threat Detection, Anomaly Detection, and Network Security**

I. INTRODUCTION

The complexity and scale of modern networked systems have been enormously increased by the introduction of new digital technologies, Cloud Computing, and the IoT [1]. Although these advancements have made connectivity and exchange of data flow smoothly, they have also increased the attack surface by cyber threats [2]. Malware, DoS attacks, breaches of data, and unauthorized access attempts are all malicious activities that have continued to evolve to a high level, causing severe threats to critical infrastructures, organizations, and individual users. Subsequently, effective cybersecurity has even become a priority issue for the industry and academia.

IDS systems are important in network protection by tracking the traffic and detecting any suspicious activity. The legacy IDS methods that are mainly signature matching and rule-based detection methods detect only known threats and not novel or zero-day attacks [3][4]. Furthermore, manual analysis is not feasible in the present world where the volume and velocity of the network data are immense [5]. These constraints have inspired incorporating the Artificial Intelligence (AI) methods in intrusion detection to allow automated, adaptive and scalable security solutions.

AI-based IDS are based on ML and DL algorithms and studies and processes complex network traffic patterns, differentiates between normal and anomalous behaviour, and identifies new attacks [4][6]. These systems can continuously learn on the basis of data, and improve detection accuracy and human intervention [7]. Still, there are problems of data imbalance, high false alarms, computing time, and non-interpretability that make them not easy to apply to real-life settings.

The paper provides a detailed literature review of AI-based IDS, the tools, the methods, and the problems associated with their development and use. The assignment is to analyze the existing practices, describe their strengths and weaknesses and identify unanswered gaps in the study that need to be filled to work out powerful and efficient fifth-generation cybersecurity systems.

A. Organization of the paper

This is the outline for the rest of the paper: Section II introduces AI-based IDS for cybersecurity, including types, detection approaches, and AI-driven techniques. Section III discusses the tools and platforms enabling AI-driven IDS, such as machine learning frameworks, AI-integrated security tools, big data streaming platforms, and cloud-based solutions. Section IV examines major challenges, including noisy data, computational overhead, adversarial threats, and limited real-world deployment. Section V reviews recent studies in the field, highlighting key methodologies and performance trends. Finally, Section VI summarizes the paper's key results and future study prospects.

II. AI-BASED INTRUSION DETECTION SYSTEMS FOR CYBERSECURITY

IDS Network-based (NIDS) and host-based (HIDS) are important security systems that identify unauthorized access, malicious activities and abnormal behaviour in the computer

systems and computer networks. These systems constantly survey the traffic and system occurrences so as to identify possible intrusions and as such, assist organizations in safeguarding sensitive information, system integrity and discourage security attacks. AI-based IDS supplement the traditional detection ability by using ML and deep learning to process extensive amounts of network interactions. They are able to recognise suspicious behaviour like suspicious data transfers, malware, and unauthorised logins, even of hitherto unidentified types of attacks [8]. On identifying any possible threats, the IDS produce real-time warnings and extensive logs, which allow responding promptly to such incidents and conducting a forensic investigation. Besides the detection of threats, IDS also help in ensuring regulatory compliance since they have records indicating the activities conducted in the network which may be required during the security audit.

A. Types of IDS

There are many types of IDSs, which can be summarized as follows:

1) Host-based IDS (HIDS)

The purpose of an IDS that is host-based is to keep tabs on a specific host's system activities and identify any attempts to compromise it. Data forensics, statistical analysis, access control, statistical assistance, and centralized audit policy administration are all features of powerful technologies. Internal threats and aberrant behaviours within local networks are most effectively addressed by host-based intrusion detection, which is capable of monitoring and responding to specific user actions and file access on the host [9][10]. A significant proportion of computer hazards originates from concerns. In contrast to host-based IDS, which relies on a single system, all machines save audit log information. Intruders may alter audit records and modify IDS binaries after they take over a system.

2) Network-based IDS (NIDS)

The use of "packet sniffers" and other methods for monitoring data transmissions between hosts is important to NIDS. The IDS in the network captures data as it travels via different channels and protocols. The protocol TCP/IP is primarily employed. In this case, the packets are captured and analyzed using a variety of methods. Packets are compared to a signature database by numerous network-based intrusion detection and prevention devices [11]. This verifies whether it contains any harmful packets or known assaults. It also looks at the packet's activities, which might indicate bad actors were involved in a certain transaction. NID is best understood as a border resistance in any scenario. Network Intrusion Detection (NID) focuses on data sent between hosts, while host-based intrusion detection pays more attention to events occurring on the hosts themselves.

3) Hybrid-based IDS or mixed IDS (MIDS)

The ability to control and receive alerts from both host-based and network intrusion detection sensors is a key feature of hybrid IDS. Hybrid systems provide the best central intrusion detection management solution when paired with NID and HID. Cisco has developed a module for the Catalyst 6000 switch that solves the first of these problems by incorporating network intrusion detection right into the switch. Aside from that, the Internet Security System (ISS) Network has shown its ability to sniff packets at gigabit rates.

B. Detection Approaches

The security of the IoT networks, which include a vast array of devices and applications, relies heavily on IDS. Traditional IDS may be broadly classified into three types:

1) Signature-based detection

The signature-based IDS detect attacks through a comparison with a database of known attack signatures or patterns. This technique is very capable with the previously known attacks and high false positive rate is usually low thus it is considered dependable in normal security processes [12]. But it is not effective against new, unknown, or zero-day attacks that do not correspond to existing signatures. Additionally, maintaining a current signature database may be challenging since it has to be updated and maintained on a regular basis. In dynamic IoT environments, new threats are emerging at an alarming pace.

2) Anomaly-based detection

A profile of typical system or network activity is created by the IDS based on anomalies, and any notable differences are flagged as potential intrusions. The method can identify any unidentified attacks and the variations of known dangers and therefore it is useful especially in a changing threat environment [13][14]. The impact of this is that anomaly-based systems have a high FPR, even if the behaviour that is being detected is legitimate but not usual, and is therefore wrongly considered malicious. Moreover, a correct definition of normal behaviour would require a lot of training data, which could be challenging to get for resource-limited or highly dynamic IoT systems.

3) Specification-based detection

Specification-based IDS takes an integrative approach of signature-based and anomaly-based. It is based on a set of predefined rules or specifications that constitute proper behaviour of the system, which are usually based on protocol specifications, application requirements or expert knowledge. Anything that contravenes these specifications is considered suspicious [15][16]. This methodology is able to identify unknown attacks of the past, and the false positive rates are lower than those of systems that use purely anomaly-based systems. Nevertheless, the process of creating a detailed and precise specification is lengthy and needs an extensive understanding of the domain. Also, it can be difficult to maintain these specifications as systems evolve, particularly in very large or diverse IoT contexts.

C. AI-Based Intrusion Detection Techniques

Artificial Intelligence (AI) has achieved massive improvements in IDS to be automated, adaptive, and accurate in detecting cyber threats, especially in a dynamic system like the Internet of Things [17]. ML and DL are the major tools used by AI-based IDS to distinguish between legitimate and malicious network activity, thereby detecting both known and new threats.

1) Machine Learning Approaches

Many machine learning-based AI-driven IDS solutions are based on machine learning techniques. Such methods get to know patterns based on network traffic information and label activities as either benign or malicious.

a) Supervised Learning

Supervised algorithms are trained on Labelled Datasets where each occurrence is labelled as either attack traffic or

normal. The model can correctly categorize fresh data once it has been trained [18]. Common supervised techniques used in IDS include DT, SVM, RF, and KNN. These methods are effective when high-quality labelled data is available.

b) Unsupervised Learning:

Labelled sets of training data are used to train supervised algorithms where every item is identified as either normal or attack traffic. The model can also accurately classify new observations after training. Some of the common techniques used in the IDS that are supervised are Decision Trees, SVM, RF, and KNN. Such techniques work well when the available data has high-quality labels.

c) Semi-Supervised Learning

A big collection of UnlabeledData is used in training together with a small set of LabeledData in semi-supervised learning. This hybrid strategy is utilised in co-training and semi-supervised SVM algorithms to improve detection performance in situations with a limited amount of labelled data. This approach is particularly applicable in the practice setting where high-quality labelled cybersecurity information is hard to get.

2) Deep Learning Approaches

Deep learning technologies build on classic machine learning methods by permitting the extraction of rich features with a lot of data automatically and with a high level of scale, thus being very efficient when it comes to sophisticated intrusion detection.

a) Artificial Neural Networks (ANN)

ANNs are human brain-inspired computational models that have the ability to learn nonlinear relationships and other Complex Patterns in Network Traffic. Feedforward neural networks are normally applied in classification activities in IDS.

b) Convolutional Neural Networks (CNN)

CNNs have found new uses outside their initial image processing applications, such as intrusion detection using structured data derived from network traffic. CNNs can detect cyberattacks even in their most subtle forms because of their superior ability to understand spatial patterns and correlations.

c) Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM):

RNNs may be used to track time-dependent Network Traffic as they are sequential data analyzers. The ability of specialized RNNs and LSTM networks to learn time series and long-term dependencies is crucial for identifying subtle or sluggish assaults that evolve over time.

Table I is a review of the current research on AI-based IDS and highlights multiple ML and DL models, datasets, strengths, limitations, and reported performance indicators. The comparison reveals that hybrid and deep learning models tend to reach a higher detection accuracy though they usually demand significant computing capabilities [19][20]. In general, the table gives a brief summary of the current innovations and trade-offs associated with designing effective IDS solutions

TABLE I. RELATED WORKS ON INTRUSION DETECTION

Method / Model	Dataset Used	Key Advantages	Limitations
Artificial Neural Network (ANN)	Custom event profiles dataset	Effective for event-based threat detection	Limited generalisation to unseen attacks
CNN–LSTM (Hybrid DL)	NSL-KDD, UNSW-NB15	Supports real-time detection and captures spatial–temporal features	High computational cost
ML & DL Techniques (Survey Study)	Various IoT datasets	Comprehensive comparison of existing approaches	No new model implementation
Generative Adversarial Network (GAN)	CICIDS2017	Improves detection using adversarial training	Complex and resource-intensive training
Multi-Layer Perceptron (MLP)	CICIDS2017	Supports explainability using XAI techniques	Limited suitability for real-time systems
Convolutional Neural Network (CNN)	UNSW-NB15	Efficient feature extraction for large datasets	Limited ability to capture temporal dependencies
Hybrid Deep Learning Model	NSL-KDD, UNSW-NB15	Effective against diverse attack types	Scalability issues for very large data
Hierarchical Spatial–Temporal Model	NSL-KDD, UNSW-NB15	Captures both spatial and temporal relationships	Requires extensive hyperparameter tuning
CNN + BiGRU	CICIDS2017	Combines spatial and sequential analysis	High memory and processing requirements
LSTM Network	NSL-KDD, CICIDS2017	Strong performance on sequential traffic data	Risk of overfitting with limited data
CNN Model	NSL-KDD, UNSW-NB15	Effective classification performance	Weak handling of time-dependent patterns

III. TOOLS AND PLATFORMS FOR AI-DRIVEN IDS

The most applicable tools/platforms that render AI-based IDS are the ML frameworks, AI-enhanced security applications, streaming big data technologies, and cloud-based intrusion detection systems. It explains the cooperation of these elements in providing data processing on a large scale, real-time surveillance and intelligent threat detection in modern network environments. On the whole, this section lays emphasis on the technological basis that is needed to construct scalable, precise, and responsive AI-based cybersecurity systems.

A. Machine Learning Frameworks

Machine learning systems assist in the construction of, teaching, assessing, and releasing Artificial Intelligence models in an intrusion detection system. These frameworks provide existing algorithms, optimization applications and scalable infrastructure to help researchers and practitioners create effective AI-based security solutions.

1) TensorFlow

TensorFlow is an open-source deep learning system that is useful in running large-scale numerical computation and machine learning. It fosters training on many devices, the

effective management of large-scale data, and the application in production [21]. The popularity of TensorFlow in intrusion detection research specifically is due to its scalability and rich ecosystem, where it may be utilized to produce deep neural networks (convolutional and recurrent). Fig. 1: A TensorFlow workflow of an AI-based IDS reflecting the concepts of training on processed network traffic data and running the saved model in cloud, edge, and real-time security systems

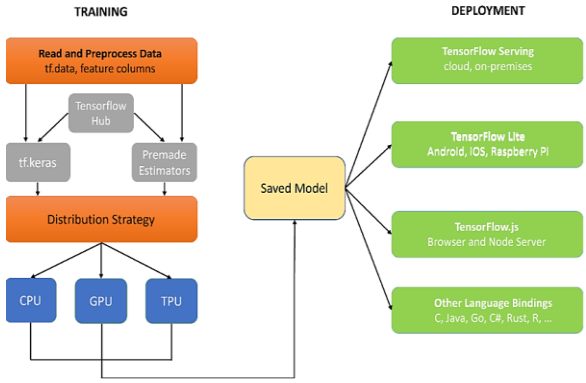

Fig. 1. TensorFlow architecture

2) PyTorch

PyTorch is a popular DL framework that is characterized by a flexible nature and dynamically compiled computation graph that enables models to be changed at runtime. This is a characteristic that makes it especially useful to experimental research and quick development of sophisticated structures. PyTorch finds wide application in IDS research in implementing advanced algorithms e.g. LSTM, GRU, and hybrid deep learning-based methods of network traffic sequence analysis.

3) Scikit-learn

Scikit-learn is a widespread Python package that deals with classical machine learning. It offers effective executions of algorithms including DT, SVM, RF, clustering algorithm and anomaly algorithm. It is also very common in intrusion detection research to use Scikit-learn as a baseline IDS model, feature selection, and comparison testing due to its simplicity and good performance on structured data.

B. Security Tools with AI Integration

Artificial Intelligence (AI) coupled with security tools can be important in improving the performance of the IDS. These technologies enable dynamic response, threat detection and automated monitoring by inspecting large volumes of network traffic and identifying suspicious patterns [22]. Conventional security measures along with AI can help organizations to design improved detectives, reduce false alarms, and respond faster to emerging cyber threats.

AI-powered security tools also enable ongoing risk assessment and system security monitoring throughout the lifecycle of the system operation. They help in detecting sophisticated attacks, including threats that never existed, using the help of ML models, which are trained on the normal and malicious network activities [23]. Additionally, the tools can support incident tracking, the development of alerts, and forensic investigations, which will improve the overall network protection.

The newer IDS platforms are also adding predictive analytics and anomaly detection features so that they can now predict the occurrence of intrusions rather than just react to established signatures. The fact that explainability features are integrated also increases the level of trust and usability because it makes the security analysts understand the reason why a certain event was raised as malicious. In general, AI-enabled security solutions offer proactive, scalable, and intelligent solutions to protect infrastructures of the network against emerging cyber-attacks.

C. Big Data and Streaming Platforms

AI-based IDS rely on big data and streaming platforms since the modern network generates large amounts of high-speed traffic, which need to be collected, processed, and analyzed in real time [24]. Such platforms will offer scalable data pipelines, distributed processing services, and effective monitoring tools, which may be used towards intelligent threat detection.

1) Apache Kafka

The ApacheKafka platform is a Distributed Streaming system that can handle massive amounts of data instantly. A publish-sub Messaging Service and a pub/sub Messaging System are the backbone of an ApacheKafka cluster, enabling producers to publish content on Kafka topics and consumers to subscribe to these topics to receive new content as it becomes available. A producer in Kafka is one that publishes data to Kafka topics [25][26]. Data may be published in a variety of formats, including text, binary, and even JSON. A producer will transmit a message with a key and a value when it publishes data to a Kafka topic. The message can be identified using the key and also partitioned and indexed. The actual data is contained in the value.

2) Apache Spark

The Apache Spark ecosystem has a large number of available libraries and modules that can be used to augment its functionality in various areas. Spark SQL gives users the ability to easily mix SQL statements with Spark programs, which means that they can use their SQL knowledge to query structured data. Spark streaming is made to handle real-time data processing, and thus it is applicable in low-latency analytics applications [27][28]. MLlib can offer machine learning algorithms that are scalable, enabling data scientists and analysts to perform data mining and analysis of large volumes of data. GraphX builds on the Spark platform by allowing the processing of graph-structured data, and allows the exploration of multifaceted relationships in data. Apache Spark has been integrated with other technologies such as Hadoop and Kafka to become a viable option to those organizations seeking to leverage big data in multiple data sources and processing environments

3) ELK Stack

ELK Stack is a common log management system, data analysis and visualization tool, which is applied in cybersecurity applications. Logstash collects and preprocesses data from different sources, Elasticsearch caches and indexes the data so that it can be easily accessed, and Kibana is the one that provides interactive dashboards to observe and explore security events. ELK can enable centralized logging, real-time analysis and visualization of the threats in IDS environments, which is an effective method to conduct an incident response

D. Applications and Challenges of Cloud-Based IDS and Threat Detection

Because of the remote, ever-changing, and massively scalable character of cloud settings, IDS have become a

necessary part of today's cybersecurity landscape. Threat detection has been greatly enhanced in terms of accuracy, flexibility, and real-time capabilities with the integration of cloud-based IDS with AI, ML, and DL [29][30]. This section discusses the primary uses and major obstacles of modern cloud-based IDS, as well as their development and implementation.

- Real-Time Threat Detection Continuous monitoring of large, fast-moving data streams produced by APIs, containers, and virtual machines is made possible with cloud-based IDSs. Using real-time analytics, these systems may quickly identify abnormalities, zero-day assaults, and the spread of malware.
- Multi-Tenant Security Monitoring By providing many customers with scalable, segregated detection capabilities, cloud IDS enables multi-tenant systems. This enables CSPs to use role-based access and specific rules to create shared yet secure IDS systems.
- Integration with DevSecOps Pipelines It is possible to enforce security regulations across the development and deployment stages by integrating modern cloud-based IDS technologies into DevSecOps processes. Security is not compromised in the process of supporting continuous integration and continuous delivery (CI/CD).
- Data Privacy and Confidentiality There are a number of issues that might arise from the processing of sensitive data by IDS systems in the cloud, including data protection, compliance with regulations (such as GDPR and HIPAA), and breaches of confidentiality. The complex issue of preventing intrusion detection from violating tenant data sovereignty continues.
- Encrypted Traffic Analysis The capacity of cloud-based IDS to examine packet contents is being hindered by the widespread use of encryption protocols, such as TLS 1.3 and VPNs. Despite ongoing research, advanced methods like TLS fingerprinting and metadata analysis are still in their early stages of development.
- Adversarial Machine Learning The use of maliciously constructed inputs to trick ML-based IDS models is known as an adversarial attack. Concerns about the security of AI pipelines and the need to strengthen models to withstand poisoning and evasion attempts are on the rise

IV. Challenges in AI-Based IDS

Intrusion detection has greatly increased in terms of level of accuracy and automation of threats with the help of AI. However, AI-based IDS also have a number of threats to its effectiveness, especially in the dynamic and complicated network environment. These issues are caused by the constraints in evaluation practice, the quality of data, computer efficiency, and practicality in the field.

A. Multiple Concurrent Attacks are difficult to detect

AI-based IDS are usually very accurate at identifying a single type of attack, but can be reduced in performance in cases of multiple attacks at once or different characteristics of the attacks [31]. Most of the models are only focused on accuracy, ignoring other vital performance measures.

Solution: Establish assessment systems that take into account holistic measures like F1score, False Acceptance Rate (FAR), precision and recall besides accuracy. Tradeoffs among various measures enhance the capability of the system to identify various threats that are multiple and simultaneous.

B. Performance Degradation because of Noisy Data

Published intrusion detection records tend to be large and may contain noise, redundant or irrelevant information. Such data can impact the training of the models negatively according to lower accuracy and overtraining.

Solution: Apply heavy techniques of preprocessing like noise dropping, outliers, feature selection and data cleaning. These processes improve the Data Quality and model generalizability.

C. Recklessness with Computational Efficiency

The majority of AI-based IDS systems do not cover such practical limitations as time complexity, CPU consumption, and processing overhead [32]. In resource-constrained settings real-time detection and deployment can be impaired by the processing requirements.

Solution: Design a lean and mean solution that takes into account the cost of the computations during the design. The processing time and resource consumption can significantly improve the real-time applicability of the process.

D. Not deployed in the real world

Although the IDS and IPS are a significant body of research, only a few AI-based solutions have ever been experimented in real-life operation conditions. It is a loophole that does not give credibility to their strength in transforming cyber threats.

Solution: Test and develop IDS frameworks on the basis of real network traffic and implementation. Pilot projects and field tests may facilitate bridging the gap between cybersecurity research and practice of this new knowledge in the real world

V. Literature Review

Table II offers a summary of existing research on AI-based IDS by comparing various studies and highlighting their objectives, methods, uses, constraints, and research opportunities. It shows that advanced ML and DL algorithms improve real-time threat detection in cloud, IoT and 5G scenarios, but there are still problems, such as a high complexity of computations, weak explainability and no detection of zero-day attacks.

H. M. Rai, A. Pal, R. A. Ergash O'g'li, B. A. Kholmirzokhon Ugli et.al. (2025). Construction of NIDS and the revolutionary possibilities of AI. Even AI-enhanced NIDS can use ML approaches to react instantly to both known and unknown threats in real time. Supervised and Unsupervised Learning techniques together enable the system to draw the line between the normal and aberrant network activity, instead of adhering to a set of pre-existing rules. DL architectures like RNN also serve to increase the system's accuracy and adaptability [1].

F. Wang and S. Xie (2025) study the formulation and testing of sophisticated ML models of Intrusion Detection on the cloud. They compare the performances of the traditional GNNs and CNNs, LSTMs, Isolation Forests, and Transformer-based Spatio-Temporal Graph Neural Networks (ST-GNNs) on the 3 distinct datasets NSL-KDD, CICIDS2017 and their own synthetic dataset. Some of the key measures used to measure the models were prec, recall,

F1score, ROC-AUC and Detection Latency. According to their results, ST-GNN built on Transformers is a very promising future IDS due to its high performance, scalability, and efficiency on real-time detection [33].

E. N. Amachaghi, M. Shojafar, C. H. Foh, et. al. (2024) evaluate past studies and case studies to illustrate why IDS are important in detecting and averting security attacks in Open RAN systems. They clarify the unique obstacles that Open RAN's disaggregated architecture introduced and categorise them as technical and non-technical threats. Lastly, they deliberated on a series of recent developments that are acquiring momentum in the Open RAN security domain and offered suggestions for future research directions [34].

K. Dhanushkodi and S. Thejas (2024) analyzes the function of AI in strengthening cybersecurity and threat detection, with an emphasis on current strides and persistent obstacles in this ever-changing domain. Cybersecurity risks such as zero-day vulnerabilities, Adversarial Assaults, and Network Breaches may now be more effectively detected and mitigated with the use of AI, particularly ML and DL approaches. Findings highlight the significance of AI model explainability and resilience in establishing trustworthiness and dependability of AI-based security solutions. The reviewed examples cover a huge range of industries, including Industry 5.0, IoT, 5G networks, and autonomous vehicles that show how AI can be applied to specific security concerns in these sectors. Efforts are underway to improve the accuracy and timeliness of Threat Detection Systems using cutting-edge techniques like Blockchain Integration, Federation Learning, and transformer-based models [35].

M. Markevych and M. Dawson (2023) give a brief overview of IDS and AI and analyze the literature on the subject matter, highlighting the necessity of applying advanced language models to enhance cybersecurity. The research provides the methodology for testing the effectiveness of AI in IDS. Also, in an effort to offer a comprehensive evaluation, the study considers such critical performance metrics as detection accuracy, FPR and response time. Research shows that AI can greatly improve its ability to identify and counteract cyberattacks [36].

P. Vanin et al (2022) explain IDS and give a classification system for ML techniques. The main criteria used to assess an IDS are presented in this article, followed by a review of modern IDS that have employed machine learning and an explanation of the benefits and drawbacks of each approach. The accuracy of the conclusions drawn from the assessed study is then discussed, together with details on the different datasets used in the investigation. Lastly, future trends, research problems, and observations are presented. Moreover, zero-day assaults are difficult for many IDS to identify. Researchers have recently taken to using ML techniques for fast and accurate network intrusion detection [37]

TABLE II. LITERATURE REVIEW TABLE: AI-DRIVEN INTRUSION DETECTION SYSTEMS (IDS)

Authors (Year)	Focus/Objective	Approaches	Applications	Limitation	Future Work
Rai et al. (2025)	Development of AI-enhanced NIDS capable of detecting known and unknown threats	Machine Learning (Supervised & Unsupervised), Deep Learning (RNN)	Real-time network security monitoring and anomaly detection	Limited interpretability of deep models; potential high computational cost	Improve explainability, scalability, and deployment in large-scale networks
Wang & Xie (2025)	Evaluation of advanced MLmodels for intrusion detection in Cloud Environments	Transformer-based ST-GNN, CNN, LSTM, Isolation Forest, GNN	Cloud security using datasets NSL-KDD, CICIDS2017, Synthetic dataset	Complex architecture, high training time and resource requirements	Optimise models for faster detection latency and real-world deployment
Amachaghi et al. (2024)	Analysis of IDS role in securing OpenRAN architectures	Literature review, threat classification, case studies	Security of OpenRadioAccess Networks (5G/Open RAN)	Lack of standardized security frameworks for Open RAN	Development of robust IDS tailored for disaggregated network environments
Dhanushkodi & Thejas (2024)	Role of AI in modern cybersecurity threat detection	ML, DL, Transformer models, Federated Learning, Blockchain integration	IoT, Industry 5.0, 5G, Autonomous Vehicles	Challenges in explainability, robustness, and adversarial resilience	Research on trustworthy AI, resilient models, and privacy-preserving security systems
Markevych & Dawson (2023)	Review of AI integration in IDS and impact on cyber-attack detection	AI models including advanced language models; performance evaluation metrics	General cybersecurity and intrusion detection	High false positive rates in some AI systems	Improve accuracy and response time; reduce false alarms
Vanin et al. (2022)	Taxonomy of ML methods for IDS and review of datasets and metrics	ML techniques for intrusion detection	Network intrusion detection across various environments	Difficulty detecting zero-day attacks; dataset limitations	Development of IDS capable of handling unknown attacks and evolving threats

VI. CONCLUSION AND FUTURE WORK

The IDS based on AI has greatly revolutionized cybersecurity as it can detect malicious activities in a complex and dynamic network environment in a precise, adaptive and real-time manner. AI-based IDS may identify both known and unknown assaults, including zero-day threats, by combining traditional detection techniques with ML and DL solutions. With the help of advanced tools, big data platforms, and cloud technologies, scalability, automation, and continuous monitoring are further enhanced. However, it has some drawbacks such as demanding computational resources, unbalanced and noisy data, vulnerability to adversarial examples, and the inability to analyze encrypted traffic and inadequate real-life usage. To overcome this, there ought to be a higher quality of data, model conception, appraisal metrics, and a higher price of being linked with functioning security systems. Overall, AI-based IDS is a highly significant part of the existing policy of protection, which is both proactive and intelligent in the implementation of the protection on a Large Scale, though it should be further investigated and tested in practice to reach high reliability.

Next-generation research should focus on explainable and lightweight AI models that can be implemented in real-time to function in resource-constrained situations, like the IoTs and edge networks. The next generation intelligent approach to cybersecurity will be made more reliable, scalable and confident by developing new resistant approaches to adversarial attack, automated analysis of encrypted traffic and verification of the IDS on real-world data

REFERENCES

[1] H. M. Rai, A. Pal, R. A. Ergash o'g'li, B. A. Kholmirzokhon Ugli, and Y. S. Shokirovich, "Advanced AI-Powered Intrusion Detection Systems in Cybersecurity Protocols for Network Protection," *Procedia Comput. Sci.*, vol. 259, pp. 140–149, 2025, doi: 10.1016/j.procs.2025.03.315.

[2] T. A. Khan *et al*., "Multi-Source Cyber Intrusion Detection Using Ensemble Machine Learning," *J. Comput. Sci.*, vol. 21, no. 1, pp. 111–123, Jan. 2025, doi: 10.3844/jcssp.2025.111.123.

[3] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, *Advancing cybersecurity: a comprehensive review of AI-driven detection techniques*, vol. 11, no. 1. Springer International Publishing, 2024. doi: 10.1186/s40537-024-00957-y.

[4] S. Kumar, S. Gupta, and S. Arora, "Research Trends in Network-Based Intrusion Detection Systems: A Review," *IEEE Access*, vol. 9, pp. 157761–157779, 2021, doi: 10.1109/ACCESS.2021.3129775.

[5] S. B. Shah, B. Boddu, N. Prajapati, and S. A. Pahune, "AI-Powered Advanced Intrusion Detection for Securing Cloud Environments Against Network Attacks," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–7. doi: 10.1109/GINOTECH63460.2025.11076673.

[6] N. Prajapati, "The Role of Machine Learning in Big Data Analytics: Tools, Techniques, and Applications," *ESP J. Eng. Technol. Adv.*, vol. 5, no. 2, pp. 16–22, 2025, doi: 10.56472/25832646/JETA-V5I2P103.

[7] M. Hana, I. Aouraghe, O. El Haouari, G. Khaissidi, and M. Mrabti, "A Survey of Artificial Intelligence Techniques in Intrusion Detection for the Internet of Things," *J. Eur. Des Systèmes Autom.*, vol. 58, n°. 6, pp. 1189–1196, juin. 2025, doi: 10.18280/jesa.580609.

[8] H. P. Cyril, "DeepNetDetect: A Deep Learning-Based Approach for Early Anomaly Detection in Network Traffic," in *2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC)*, IEEE, Feb. 2026, pp. 1–6. doi: 10.1109/ICAIC67076.2026.11395734.

[9] A. Das and P. S. Sharma, "A Survey on Intrusion Detection System Types and Techniques," *Int. J. Sci. Eng. Technol.*, vol. 11, no. 4, pp. 928–932, 2023.

[10] G. Sarraf and V. Pal, "Adaptive Deep Learning for Identification of Real-Time Anomaly in Zero-Trust Cloud Networks," *ESP J. Eng. Technol. Adv.*, vol. 4, no. 3, 2024, doi: 10.56472/25832646/JETA-V4I3P122.

[11] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *TIJER--Int. Res. J*, vol. 9, no. 10, pp. 49–55, 2022.

[12] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, p. 18, Mar. 2021, doi: 10.1186/s42400-021-00077-7.

[13] S. Ferozuddin and S. W. A. Rizvi, "AI-Driven Anomaly Detection Model for Intrusion Detection Systems (IDS)," *Int. J. Comput. Appl.*, vol. 187, no. 6, pp. 51–55, May 2025, doi: 10.5120/ijca2025925093.

[14] D. Shah, S. Khade, and S. Pawar, "Anomaly Detection in Time Series Data of Sensex and Nifty50 With Keras," in *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, IEEE, Mar. 2021, pp. 433–438. doi: 10.1109/ESCI50559.2021.9396979.

[15] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.

[16] 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.

[17] S. Kakolu, M. A. Faheem, and M. Aslam, "AI-enabled intrusion detection systems in IoT networks: Advancing defence mechanisms for resource-constrained devices," *Int. J. Sci. Res. Arch.*, vol. 9, no. 1, pp. 752–769, Jun. 2023, doi: 10.30574/ijsra.2023.9.1.0316.

[18] D. Bhattacharjee, "Design and Evaluation of Deep Generative AI Model for Intrusion Detection in Cyber Threat Monitoring," in *2025 7th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*, 2025, pp. 1–6. doi: 10.1109/ISAECT68904.2025.11318752.

[19] A. Nizam, A. Prakash, A. S, H. Mohan, and A. Mehar, "A Comparative Study on AI-IDS Artificial Intelligence-Based Intrusion Detection System," *IJERT*, vol. 14, no. 2, 2025, doi: 10.5281/zenodo. 18114700.

[20] 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.

[21] M. Ramchandani *et al.*, "Survey: Tensorflow in Machine Learning," *J. Phys. Conf. Ser.*, vol. 2273, no. 1, 2022, doi: 10.1088/1742-6596/2273/1/012008.

[22] S. Narula, M. Ghasemigol, J. Carnerero-Cano, A. Minnich, E. Lupu, and D. Takabi, "Exploring Research and Tools in AI Security: A Systematic Mapping Study," *IEEE Access*, vol. 13, pp. 84057–84080, 2025, doi: 10.1109/ACCESS.2025.3567195.

[23] R. V. S. S. Bharattej R, Y. M. M. John, M. Bai. 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.

[24] M. Shahnawaz and M. Kumar, "A Comprehensive Survey on Big Data Analytics: Characteristics, Tools and Techniques," *ACM Comput. Surv.*, vol. 57, no. 8, pp. 1–33, Aug. 2025, doi: 10.1145/3718364.

[25] M. Singh, N. Bhardwaj, R. Sringhi, and L. Vashistha, "A Comprehensive Study on Big Data Processing with Apache Spark," *Int. J. Sci. Res. Eng. Trends*, vol. 10, no. 2, pp. 447–449, 2024.

[26] A. R. Toorpu, S. K. Vududala, A. Nerella, and B. P. Madupati, "Hybrid AI Models for Privacy-Preserving Big Data Analytics in Distributed Environments," in *2025 Global Conference in Emerging Technology (GINOTECH)*, IEEE, May 2025, pp. 1–8. doi: 10.1109/GINOTECH63460.2025.11076666.

[27] W. Khalil, H. Torkey, and G. Attiya, "Survey of Apache Spark optimised job scheduling in big data," *Int. J. Ind. Sustain. Dev.*, vol. 1, no. 1, pp. 39–48, Jan. 2020, doi: 10.21608/ijisd.2020.73486.

[28] S. Singamsetty, "CyNet: Amalgam Deep Learning Model for Multi-Vector Cyber Intrusion Detection System (IDS)," in *2025 3rd International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, IEEE, Sep. 2025, pp. 914–918. doi: 10.1109/ICoICI65217.2025.11253990.

[29] S. Kumara, "A Lightweight Deep Learning-Based Classification Model 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.

[30] H. Meziane and N. Ouerdi, "A survey on performance evaluation of artificial intelligence algorithms for improving IoT security systems," *Sci. Rep.*, vol. 13, no. 1, p. 21255, Dec. 2023, doi: 10.1038/s41598-023-46640-9.

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

[32] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud

Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[33] F. Wang and S. Xie, "Cybersecurity in Cloud Computing AI-Driven Intrusion Detection and Mitigation Strategies," *IEEE Access*, vol. 13, pp. 108051–108058, 2025, doi: 10.1109/ACCESS.2025.3580569.

[34] E. N. Amachaghi, M. Shojafar, C. H. Foh, and K. Moessner, "A Survey for Intrusion Detection Systems in Open RAN," *IEEE Access*, vol. 12, pp. 88146–88173, 2024, doi: 10.1109/ACCESS.2024.3408690.

[35] K. Dhanushkodi and S. Thejas, "AI-Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access*, vol. 12, pp. 173127–173136, 2024, doi: 10.1109/ACCESS.2024.3493957.

[36] M. Markevch and M. Dawson, "A Review of Enhancing Intrusion Detection Systems for Cybersecurity Using Artificial Intelligence (AI)," *Sciendo*, vol. 3, 2023.

[37] P. Vanin *et al.*, "A Study of Network Intrusion Detection Systems Using Artificial Intelligence/Machine Learning," *Appl. Sci.*, vol. 12, no. 22, p. 11752, Nov. 2022, doi: 10.3390/app122211752.

