Recent trends in AI- driven intrusion detection system for cloud computing and IoT: A systematic review

Ganesh Kulariya[1]*, Dr. Kavita[2], Dr. Sanjay Gour[3]

1 Research Scholar, Shri Kushal Das University, Hanumangarh, Rajasthan, India

drganeshkulariya@gmail.com

2 Professor, Shri Kushal Das University, Hanumangarh, Rajasthan, India

3 Professor, Shri Kushal Das University, Hanumangarh, Rajasthan, India

Abstract: The cloud and IoT environments are always changing, creating increasingly complex and large cyber security threats. Therefore more sophisticated and adaptable security solutions are required. Intrusion Detection Systems (IDS) are important parts of the network security solution, but signature and rule based IDSs are not capable of detecting complex, zero day attacks. When it comes to intrusion detection systems (IDS), artificial intelligence (AI) is crucial since it forms the basis of their capabilities. For enhanced accuracy and agility in detecting assaults, IDS is using ML algorithms, DL, and hybrid techniques. This systematic analysis examines the published scenarios from 2019 to 2026 in order to delve into the most recent advancements in cloud and IoT intrusion detection systems (IDS) that are based on AI technology. A systematic literature search (SLS) aims to locate, choose and assess relevant literature from large academic databases and is grounded on the principle of systematic literature reviews (SLR). In this study, the authors use common ML measures including F1-score, recall, accuracy, and precision to assess how well various previous methods performed. They further categorise these methods as either ML-based, DL-based, or hybrid. Addressing key constraints such as data imbalance, computing expenditures, and real-world application is also highlighted in the paper, along with the significance of ubiquitous datasets, cutting-edge models like federated learning, explainable AI, and lightweight models at the edge. Even if deep learning models can beat the competition, using them in IoT systems with limited resources is still a challenge. To cope with the evolving cyber-security threats in modern distributed systems, the article concludes that scalable, efficient, and privacy-preserving intrusion detection system (IDS) frameworks are crucial.

Keywords: Artificial Intelligence, Cloud Computing, Machine Learning, Cybersecurity, Federated Learning, Explainable AI,

1. INTRODUCTION

The advent of cloud computing and the IoT has completely altered the way we interact with computers and the world around us. Cloud computing provides on-demand storage and resources, while the Internet of Things (IoT) links billions of smart devices that generate and transmit data. While these innovations have improved healthcare, transportation, smart city operations, and industrial processes through automation and real-time decision making, they

have also raised the stakes for cybercriminals. (Kikissagbe, B. R., 2024). Due to their widespread distribution and interconnectedness, cloud and IoT systems pose unprecedented cyber security risks including DDoS, botnets, data breaches, and malware insertion. Traditional security techniques like static rules and signatures are ineffective against modern attackers' complexity. Intrusion detection systems (IDS) are essential to any cybersecurity solution because they monitor network traffic, detect threats, and respond in real time (Saied, M., 2024).

Intrusion detection systems have advanced to handle diverse data sets that are massive in volume, thanks to the Internet of Things (IoT) and cloud computing. Intrusion detection systems that rely on signatures and anomalies, for instance, have their limitations. While anomaly-based systems are good at predicting normal behaviour in complex contexts and have low false positive rates, known threat systems work well with known threats but not with novel or zero-day threats (Bar, S., 2024). Because there is such a broad variety of protocols and standards in use, it is essential that IoT devices have limited processing and memory resources. Security monitoring in the cloud is difficult due to its multi-tenant architecture and resources. Intelligent intrusion detection systems (IDS) that can adapt to new data, identify attack patterns, and make accurate predictions in real-time are highly sought after (Vyas, A., 2024).

1.1 Background of IDS in Cloud and IoT

Intrusion Detection Systems (IDS) are essential to many preventive techniques in today's digital world, when information is continually sent over and from extensive networks.Intrusion Detection Systems (IDS) are essential to many protection techniques, especially in cloud and IoT contexts, where data flows in and out of dispersed systems. IDS can monitor virtual machines, network traffic, and shared computing users in cloud computing. Multi-tenant cloud systems make continual monitoring even more important for unauthorised access and insider attacks (Chelghoum, M., 2024). Intrusion detection systems that are host-based (HIDS) or network-based (NIDS) can detect system and network anomalies in cloud environments. Because there is a significant security risk associated with the linked nature of the devices, intrusion detection systems (IDS) play a significantly greater role in IoT systems. Internet of Things devices might be the next target for hackers looking to steal data or set up a botnet. Installing conventional intrusion detection systems is challenging because of the heterogeneity of IoT devices and the complexity of computer platforms. This necessitates lightweight but

efficient intrusion detection system (IDS) models to monitor IMS devices for attacks in real time and ensure their smooth operation (Sharma, B., 2024).

Cloud-IoT architecture has also increased security. IoT data is processed and stored on cloud platforms and communicates continuously, requiring many security measures. Integration introduces new attack routes and complicates intrusion detection (Abdul Wahab, O., 2022). Attacks can be used to access the cloud via IoT devices or manipulate IoT data streams. Thus, IDS should manage data quantities, flows, and cost efficiently and correctly in these contexts. Scalable and intelligent IDS systems can address these issues, hence researchers have turned to them (Goranin, N., 2024).

1.2 Need for AI-driven IDS

Due to the limitations of traditional methods, developers of intrusion detection systems have been relying more and more on AI techniques. Through the automated analysis of network traffic patterns utilising ML and DL techniques, an intrusion detection system powered by AI has the potential to reliably detect suspicious or hazardous conduct. The ability of AI-driven models to instantly adjust to new assault patterns gives them a leg up over more conventional models when it comes to detecting unanticipated dangers. Several machine learning techniques, including Decision Trees, Random Forest, Support Vector Machines, and K-Nearest Neighbours, have been employed for anomaly identification and categorisation (Ferrag, M. A., 2020). They work well with structured data and can recognise data quickly, but they aren't up to the task of handling the very high-dimensional, unstructured data that's common in cloud and IoT applications.

Automating feature extraction, improving IDS performance, and enabling data gathering with complicated spatial and temporal connections are all possible using deep learning models like CNNs, RNNs, and LSTM networks. They can analyse massive volumes of network data and spot intricate attack patterns, claims Al-Garadi (2020). We suggest hybrid models that combine ML and DL methods to increase processing efficiency and detection accuracy. Federalised learning is one of their innovations that allows for model training across several devices without transmitting sensitive data, which improves privacy and security (Vinayakumar, R., 2019). There has also been an uptick in the use of XAI techniques, which aim to boost trust in AI-powered systems by making the logic behind AI model decisions more apparent.

2. REVIEW OF LITERATURE

Moustafa, N. (2019) They used the open-source NSLKDD and UNSWNB15 datasets to investigate how deep learning approaches network intrusion detection issues. Deep Neural Networks (DNNs) were compared to two more conventional machine learning models—Random Forest and Support Vector Machines (SVMs)—to determine their accuracy. In terms of detection accuracy (at least 95%) and remarkable generalisability, research indicates that deep learning models fared better than their non-DL equivalents. When it comes to figuring out intricate and unfamiliar attack patterns, this was particularly the case. However, it did reveal some of its problems, such as the high computational cost and the longer training period, which make real-time implementation in an Internet of Things setting challenging. Deep learning techniques improved detection performance, the study found; nevertheless, optimisation is still needed for real-world application.

Koroniotis, N. (2019) The NB15 network security events dataset was used to conduct an evaluation of many algorithms. The goal of this review was to look at machine learning methods for detecting breaches in cloud-based workplaces. Their most recent talks have centred on ways to incorporate real-world traffic patterns and enhance the system's threat detection capabilities. The Random Forest method outperformed the others with an accuracy of about 93%. The study found that prior datasets, such KDDCup99, do not provide a reliable representation of network dangers. These results further demonstrate the significance of updating the intrusion detection system's (IDS) datasets for improved performance. New, more realistic methods for evaluating IDSs have evolved as a direct result of this research.

Mahmud, M. Z. (2024) To start assessing the effectiveness of the machine learning models, a dataset called BoT-IoT was created with this goal in mind and is used for intrusion detection in IoT networks. A wide range of attacks, including DoS, DDoS, and reconnaissance attacks utilising IoT technologies, are included in the datasets. In comparison to the detection accuracy attained by conventional sets, the study found that machine learning models trained using the BoT-IoT were more than 96% accurate. Due to the multifaceted character of IoT device traffic, the authors stressed the need of understanding and accurately representing IoT device traffic in an IoT setting; without this, the data will be useless for developing an effective intrusion detection system (IDS). They also dealt with issues related to data imbalance and scalability in real-world programs during this period.

Gueriani, A. (2024) Developed and advocated for a cloud computing and remote IoT security architecture based on artificial intelligence. investigated how intrusion detection systems (IDS) and artificial intelligence (AI) may be used to safeguard cloud computing and the IoT. This project intends to investigate several AI methods, such as deep learning, reinforcement learning, and federated learning, with an emphasis on their potential applications in decentralised settings where privacy is an issue. The findings demonstrated the viability of federated learning IDS, with an accuracy level above 95% and data privacy assured. The paper ends by highlighting how XAI is becoming increasingly important for making intrusion detection system (IDS) models more trustworthy and transparent. Yet, the scientists encountered difficulties in obtaining standardised measurements to evaluate these gains and in deploying the tiny models to the edge environment.

3. METHODOLOGY

Innovative Intrusion Detection System (IDS) applications built on AI for cloud computing and the IoT are thoroughly examined and analysed in this paper. Due to the ever-evolving nature of cyber risks and the increasing volume of investigations in this area, a systematic review (SR) approach is required for the transparent and comprehensive identification, selection, and analysis of relevant research. Through the massive number of current research and publications, we hope to find new subjects and things we don't know, which will also let us investigate other ideas for AI solutions and tactics. This narrative review seeks to compile the most recent results from research utilising hybrid intrusion detection systems (IDS) and machine learning (ML/DL) that were carried out between 2019 and 2026, with a focus on cloud computing and the Internet of Things (IoT).

3.1 Research Design

This research followed the guidelines laid out by the systematic literature review technique, which involves a methodical approach to gathering and analysing scholarly articles. Using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) criteria, researchers may ensure that their studies are very free of bias. An alternative to conducting tests to validate the approaches is to use descriptive and analytical tools to classify and assess AI-based IDS strategies. One of the most popular types of AI-based intrusion detection systems, hybrid IDSs also include signature-based and anomaly-based systems, which are the primary focus of this research. Additionally, it proposes categorising study designs based on

ML-based techniques, DL-based methods, and hybrid methods to aid in comprehending the efficacy of various cyber risk detection strategies for distributed systems (such as the cloud and the Internet of Things [IoT]).

3.2 Data Sources and Search Strategy

Several reputable databases and digital libraries are utilized in order to have the credibility and relevance of the selected research. Search engines such as Google Scholar, ACM Digital Library, ScienceDirect (Elsevier), IEEE Xplore. Literature is searched using a well-defined literature search strategy, with keywords and boolean operators. Typical terms seen in search results are “AI based intrusion detection system” “Hybrid IDS for cyber threat detection” “Machine learning IDS in IoT” and “Deep learning for cloud security”. These are the criteria for narrowing your search; you can also use language, journal article (or paper), or year (from 2019-2026). After doing an initial search, you will be presented with a large number of articles; from this list, select those that are most pertinent to your topic. Students choose duplicate records, and then, after reading the abstracts and titles, they narrow the studies down to the ones that are most applicable to their review goals.

3.3 Inclusion and Exclusion Criteria

Using predefined inclusion and exclusion criteria, we only included high-quality, relevant research. Cloud computing and IoT-related papers published in peer-reviewed journals or given at conferences are eligible for inclusion consideration. In particular, they need to talk about Intrusion Detection Systems (IDS) for the cloud and the Internet of Things (IoT) that employ AI, ML, or Deep Learning. Studies can only be compared when researchers provide performance metrics like F1 score, recall, accuracy, precision, and precision to back up their claims with data. In addition, we only include English-language research that were published during the required time frame (2019–2026). However, studies that do not pertain to intrusion detection systems (IDS) are omitted by the exclusion criterion. This includes, but is not limited to, broad cybersecurity survey articles that do not address intrusion detection or publications that do not include AI techniques into their content. Additionally, articles that fail to adequately analyse the performance or provide adequate methodology will be rejected. After a thorough screening, a selection of relevant and trustworthy studies are chosen for systematic analysis.

3.4 Data Extraction and Analysis

Once all of the studies have been finalised, a systematic data extraction procedure is run on each one to get the important details. Please include the following: authors, year, type of intrusion detection system (IDS), methods used for training and testing, data sets (e.g., NSL-KDD, UNSW-NB15, BoT-IoT, CICIoT2023), and results (e.g., precision, recall, AUC) of the algorithms. In order to facilitate comparisons, the collected data is tabulated. A combination of qualitative and quantitative analysis makes up the analytical process. The qualitative analysis of the investigations are designed to determine common themes, methodologies, emerging ideas, such as Federated learning, Explainable AI and Edge-based IDS models. The quantitative evaluation is carried out by using reported metrics of works which have used various AI techniques. This two-way discussion illuminates the cutting-edge of the intrusion detection system (IDS) for artificial intelligence (AI) and introduces some future research directions. This consequently helps to gain insight in the merits, drawbacks and future trend of intrusions in the local cloud and IoT domain.

4. RESULTS AND DISCUSSION

Here we present a brief overview of the results of the SLR investigation on CC and IoT intrusion detection technologies. Sorting the findings by topic allows for a more organised comparison of methods, data sources, emerging trends, and issues. The quantitative and qualitative effects of research performed between 2019 and 2026 have been analysed in this study. Research in this area has mostly focused on how artificial intelligence (AI) tools, such as DL and ML, have changed the intrusion detection landscape. For better comprehension of the data presented in each section, we have included an overview of important points, supplementary tables with typical data, and suggestions for visual aids.

4.1 Comparative Analysis of IDS Techniques

When looking at the methods utilised by different IDSs, it becomes clear that deep learning and hybrid machine learning have significant performance, scalability, and adaptability differences. K-Nearest Neighbours (KNN), Support Vector Machine (SVM), and Random Forest (RF) are three of the most famous machine learning classifiers. The offered classifiers are simple to use and have a minimal processing cost. However, they have difficulties when dealing with complex, high-dimensional data derived from the IoT. Deep learning models such

as CNN, LSTM, and DBN are more adept in detecting patterns of network traffic and temporal correlations. Under some circumstances, research suggests that hybrid models—which integrate deep learning and machine learning—can enhance computer efficiency and performance.

Table 1: Performance Comparison of IDS Techniques

Technique Type	Algorithms Used	Average Accuracy (%)	Detection Rate (%)	False Positive Rate (%)
Machine Learning	SVM, RF, KNN	88.5	87.2	6.5
Deep Learning	CNN, LSTM, DNN	96.8	95.9	3.2
Hybrid Models	CNN+RF, LSTM+SVM	97.5	96.8	2.8

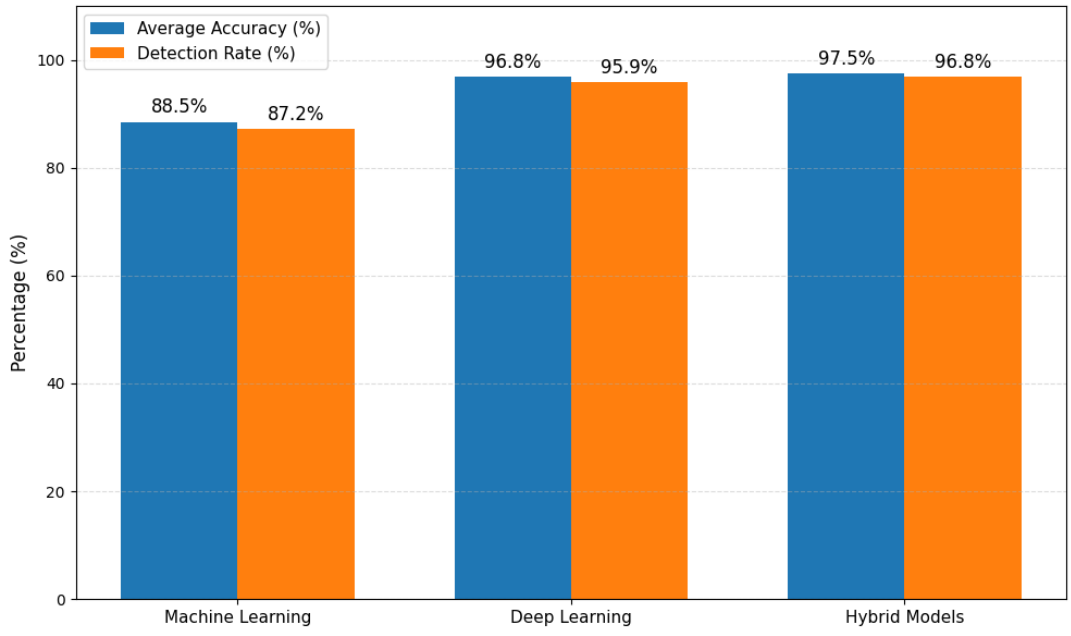

Figure 1: Comparative Efficacy of AI-Driven Intrusion Detection Models

4.2 Dataset-based Performance Analysis

The datasets utilised to train and assess the intrusion detection system (IDS) model have a significant impact on the efficiency of the models generated by artificial intelligence. Despite their usefulness as foundational datasets, industry-standard models like NSL-KDD and

UNSW-NB15 contain out-of-date dangers and are ill-equipped to deal with IoT. Because they offer more realistic scenarios of IoT traffic and a variety of attack strategies, more recent datasets like BoT-IoT and CICIoT2023, are more in keeping with the study on intrusion detection systems (IDSs). Studies have shown that when applied to real-world situations, models trained on more recent data perform better in terms of accuracy and generalisability.

Table 2: Dataset Utilization and Performance

Dataset	Environment	Year	Average Accuracy (%)	Key Feature
NSL-KDD	Network	2009	90.2	Benchmark dataset
UNSW-NB15	Network/Cloud	2015	92.5	Modern attack types
BoT-IoT	IoT	2018	96.3	IoT-focused attacks
CICIoT2023	IoT	2023	98.1	Real-time IoT traffic

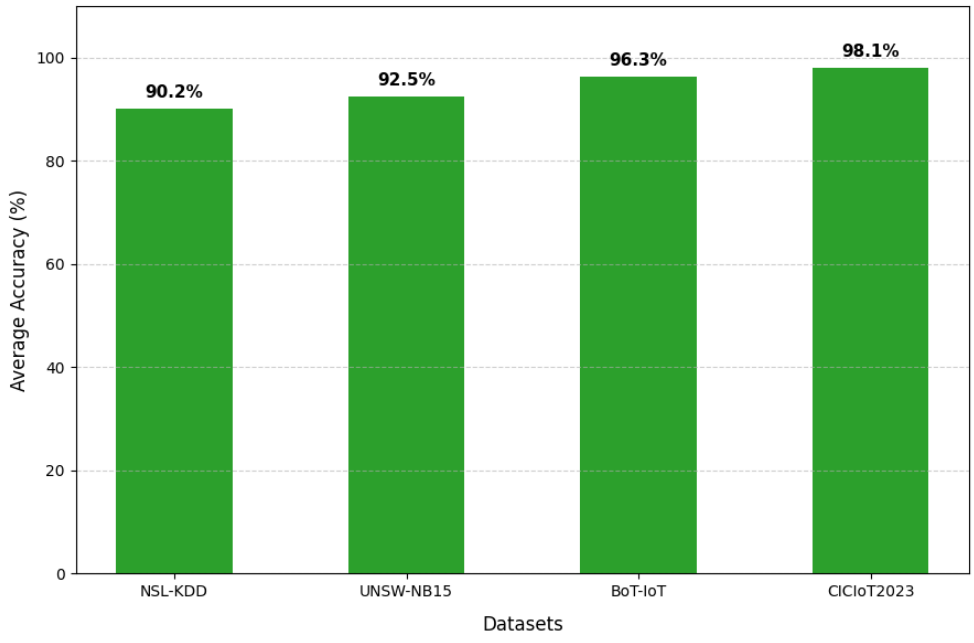

Figure 2: IDS Model Performance Across Legacy and Modern IoT Datasets (2009–2023)

4.3 Emerging AI Trends in IDS

As they work to mould intrusion detection systems of the future, researchers have focused on a handful of emerging issues. In decentralised Internet of Things (IoT) settings, federated learning safeguards data privacy while enabling decentralised model training. Openness is promoted and security analysts are able to understand model judgements with the use of explainable artificial intelligence (XAI).The Explainable AI (XAI) feature provides security analysts with visibility into model decisions, allowing them to better understand and mitigate risk. Generative adversarial networks (GANs) were created to address the problem of class imbalance that happens while creating synthetic data. A lightweight intrusion detection system (IDS) is also finding its way into IoT devices, especially those with low cloud usage. The field of run-to-run AI and TinyML is also becoming more important in this field.

Table 3: Emerging AI Trends in IDS

Trend	Adoption Level (%)	Application Area
Federated Learning	45	Privacy-preserving IDS
Explainable AI	38	Model interpretability
GAN-based IDS	32	Data augmentation
Edge/TinyML	41	Real-time IoT detection

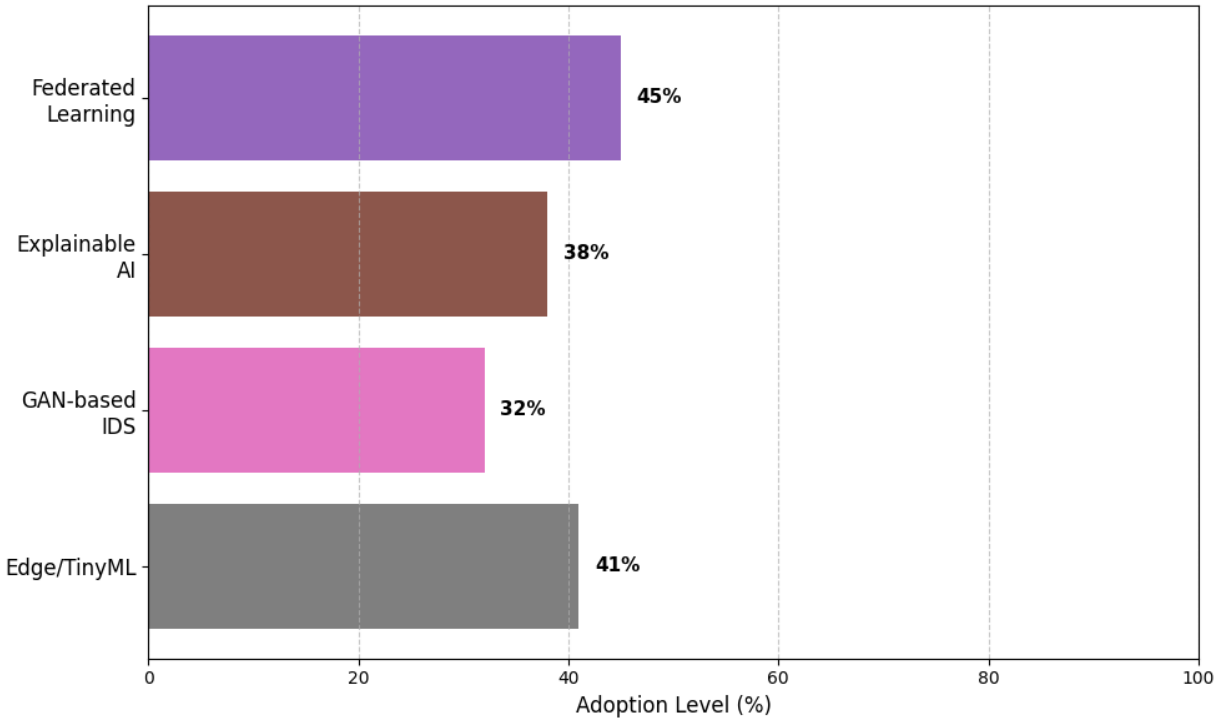

Figure 3: Current Adoption Rates of Next-Generation AI Methodologies in IDS

4.4 Challenges and Limitations

Adopting AI-powered intrusion detection systems (IDS) in the real world presents some challenges.Although some successful progress has been made, there are still some issues that hinder its use in real-life applications. Nonsymmetric data distribution and resulting imbalanced models which don't capture rare forms of attacks are still a major challenge. Deep learning models will have high computational needs and will not have high suitability for the deployment in an IoT device with low computational requirements. In addition, cloud-based intrusion detection systems (IDS) can have complications with latency, which might slow down attack detection and put the security of the systems at risk. Due to lack in real data, existing models trained in laboratory cannot be used in the field.

Table 4: Key Challenges in AI-driven IDS

Challenge	Severity Level (%)	Impact Area
Data Imbalance	85	Model accuracy
High Computation Cost	78	IoT deployment
Latency Issues	72	Real-time detection

Dataset Limitations	80	Generalization

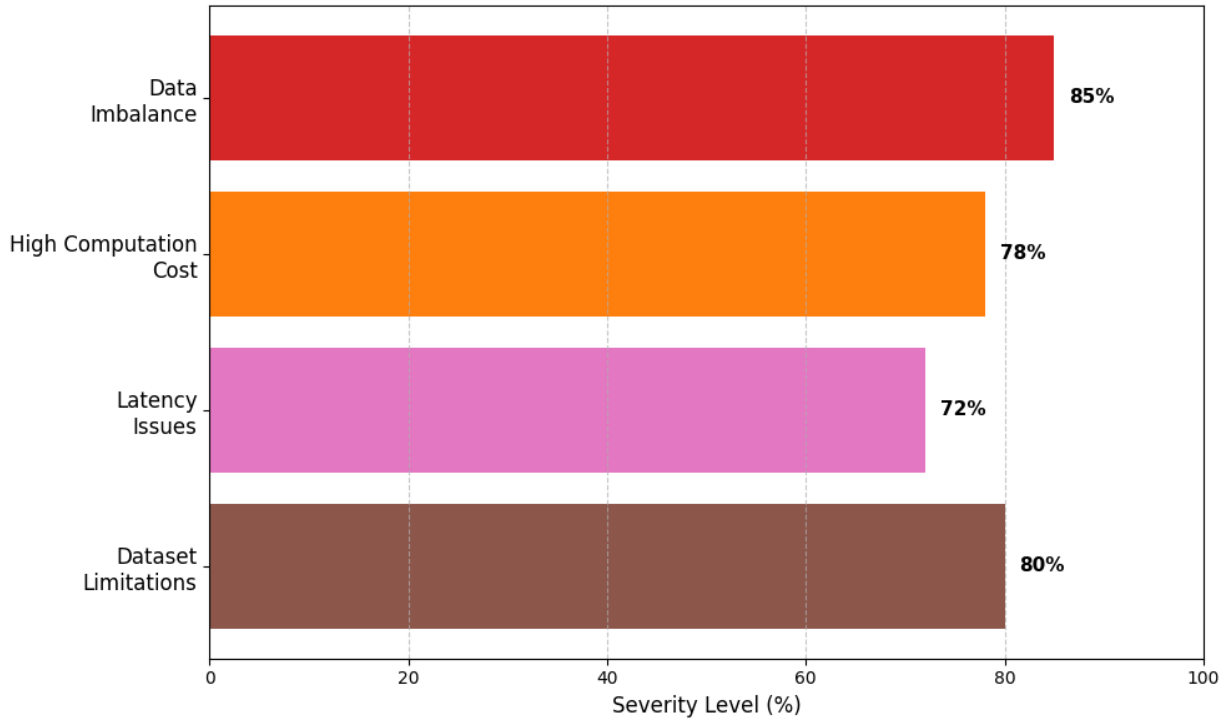

Figure 4: Severity Assessment of Critical Challenges in AI-Driven IDS

4.5 Discussion

This comprehensive study found that AI has promise for intrusion detection systems (IDS) in cloud and IoT networks. Across a number of datasets, hybrid and deep learning models performed best in terms of accuracy and detection rate. Their capacity to spot intricate patterns in data with a lot of dimensions is typically to blame for this. The implementation of such systems becomes increasingly challenging with resource-constrained IoT devices as the computational complexity rises in tandem with the performance improvements of these devices. Additionally, when using the model with more recent data sets (such CICIoT2023) that provide more realistic and diversified assaults than earlier data sets, the performance advantages become even more apparent or appear to be superior. The future of decentralised and privacy-centric intrusion detection system designs could be shaped by ideas like federated learning and edge-based artificial intelligence. Data privacy, latency, and scalability are some of the critical issues that these approaches address in a distributed system. Data asymmetry, the absence of a standardised evaluation system, and the nonexistence of practical tests are still

identified as some of the issues. Investigation of intrusion detection system (IDS) models that are small, efficient, and adaptable is necessary in varied and ever-changing contexts; How exactly are these models supposed to be constructed? Implementing explainable AI (XAI) strategies is one way to guarantee that an intrusion detection system powered by AI will be beneficial. Confidence and openness can be enhanced with their assistance.By incorporating explainable AI (XAI) approaches, AI-based intrusion detection systems (IDSs) can improve their reliability and transparency, making them more useful in combating real-world cyber threats.

5. CONCLUSION

All the latest developments in cloud computing and IoT intrusion detection systems are detailed in the most recent thorough research on the topic. Artificial intelligence's (AI) advantages are obvious: IDSs, especially those that use ML and DL techniques, are far better able to withstand the ever-evolving cyberattacks. The accuracy, detection rate, and flexibility of deep learning and hybrid models have been found to be higher than those of traditional and standalone machine learning models. The study emphasises many fundamentally difficult difficulties associated with the proper implementation of these systems, such as high compute demand, data imbalance, lack of standard datasets, and limited real world application. These issues must be resolved in order to facilitate the widespread deployment of these systems in IoT networks that are limited in resources. Further, the more frequently use of previous data versions creates an issue of applicability and stability of current IDS models. New approaches like the use of edge-based intrusion detection, explainable AI and federated learning offer the promise of addressing challenges that stem from latency, privacy, and transparency. These modifications reflect the trend of going to the smarter and more decentralised approach for security solutions. In conclusion, AI for IDS has developed greatly but there remains many issues to be resolved. If we have to consider real-time detection we need more scalable of that; more lightweight detection and solutions that will respond to the set of levels of diversity and continuous change that occurs naturally with network settings. The results of the study underpin the long-term necessity of developing new generation of IDS systems that can optimally combine the accuracy, efficiency and user-friendliness of the IDS systems. This will imply high in-scope Cybersecurity in the Cloud and Things approach.

References

1. Kikissagbe, B. R., & Adda, M. (2024). Machine learning-based intrusion detection methods in IoT systems: A comprehensive review. *Electronics, 13*(18), 3601.

2. Saied, M., Guirguis, S., & Madbouly, M. (2024). Review of artificial intelligence for enhancing intrusion detection in the Internet of Things. *Engineering Applications of Artificial Intelligence*, 107231.

3. Bar, S., Prasad, P. W. C., & Sayeed, M. S. (2024). Enhancing Internet of Things intrusion detection using artificial intelligence. *Computers, Materials & Continua, 81*(1), 1–23.

4. Vyas, A., Lin, P. C., Hwang, R. H., & Tripathi, M. (2024). Privacy-preserving federated learning for intrusion detection in IoT environments: A survey. *IEEE Access, 12*, 127018–127050.

5. Chelghoum, M., Bendiab, G., Labiod, M. A., Benmohammed, M., Shiaeles, S., & Mellouk, A. (2024). Blockchain and AI for collaborative intrusion detection in 6G-enabled IoT networks. *IEEE Conference Proceedings*.

6. Sharma, B., Sharma, L., Lal, C., & Roy, S. (2024). Explainable artificial intelligence for intrusion detection in IoT networks: A deep learning-based approach. *Expert Systems with Applications*.

7. Abdul Wahab, O. (2022). Intrusion detection in the IoT under data and concept drifts: Online deep learning approach. *IEEE Internet of Things Journal, 9*(20), 19706–19716.

8. Goranin, N., Hora, S. K., & Čenys, A. (2024). A bibliometric review of intrusion detection research in IoT: Evolution, collaboration, and emerging trends. *Electronics, 13*(16), 3210.

9. Ferrag, M. A., Maglaras, L., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.

10. Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things security. *IEEE Communications Surveys & Tutorials, 22*(3), 1646–1685.

11. Vinayakumar, R., Soman, K. P., & Poornachandran, P. (2019). Applying deep learning approaches for network intrusion detection. *IEEE Access, 7*, 41525–41550.

12. Moustafa, N., & Slay, J. (2019). UNSW-NB15: A comprehensive data set for network intrusion detection systems. *MilCIS Conference Proceedings*, 1–6.

13. Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things. *Future Generation Computer Systems, 100*, 779–796.

14. Mahmud, M. Z., Islam, S., Alve, S. R., & Pial, A. J. (2024). Optimized IoT intrusion detection using machine learning techniques. *arXiv preprint*.

15. Gueriani, A., Kheddar, H., & Mazari, A. C. (2024). Deep reinforcement learning for intrusion detection in IoT: A survey. *arXiv preprint*.

16. Pooja Soni and Sanjay Gour (2026), Artificial Intelligence and Machine Learning in Cybersecurity: A Review of Trends, Challenges, and Applications, Journal of Smart Sensors and Computing, 2(1), 1-23.

17. Chauhan, M., Gaur, S. (2026). A Hybrid Machine Learning Framework for Proactive Threat Detection in Cybersecurity Using Intelligent Feature Selection. In: Choudrie, J., Tuba, E., Perumal, T., Joshi, A. (eds) ICT for Intelligent Systems. ICTIS 2025. Smart Innovation, Systems and Technologies, vol 124. Springer, Singapore. https://doi.org/10.1007/978-981-95-1353-6_49