Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Intrusion Detection Systems: Enhancing Real-Time Network Threat Monitoring Using AI

Yousef Farhan M Alanazi

Ministry of Education, Riyadh, Saudi Arabia

Email: uo_4u@hotmail.com

ARTICLE INFO

Received: 15 Mar 2025

Revised: 21 May 2025

Accepted: 30 May 2025

ABSTRACT

The failure of the traditional intrusion detection systems has prompted the search for better options. AI-based detection systems have proved superior to the traditional intrusion detection methods. Much research has been done on these aspects. This systematic review aimed to review the current trends of research on AI-IDS for network monitoring to enhance intrusion detection. Google Scholar was used for identifying the relevant papers with appropriate search terms. The identified papers were screened, and the most suitable 20 papers were selected using the PRISMA process flow diagram. The selected papers were described in the results section and thematically analysed and their quality rated in the discussion section. There is no doubt about the superiority of AI-based intrusion detection systems. Only the components of such systems differ depending on the target of the detection system, like cloud computing, IoT or internal structures and operating systems. The challenges to the implementation of AI-based intrusion detection systems in organisations have been identified. Solutions to these have been suggested. However, how many of these solutions have been implemented successfully by any organisation is unknown. Some case studies on big and small organisations can enlighten us on this aspect. Some limitations of this review and the scope for future research have been presented.

Keywords: AI-IDS, Intrusion detection system, Network monitoring, traditional systems.

INTRODUCTION

Intrusion Detection Systems (IDS) are technologies that observe both network and user activities to detect possible cyber threats as they happen. IDS employ a variety of methods, such as examining network traffic and collaborating with other security tools, to assist in the quick identification and response to cyber threats. By adopting an IDS, businesses can gain a personalised alert system, early identification of threats, and enhanced speed in incident response.

AI-powered Intrusion Detection Systems (AI-IDS) greatly improve the monitoring of network threats in real time. These systems use artificial intelligence to recognise intricate attack patterns, conduct immediate threat assessments, and autonomously adapt to new cyber threats. AI-IDS serve as effective mechanisms for strengthening network security by proactively detecting and addressing potential cyber threats in real-time, offering an essential layer of protection against advancing cyberattacks.

Much research has been done on AI-IDS enhancing real-time network monitoring. Many reviews have also been published. This systematic review is aimed at providing the latest trends in AI-IDS,

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

enhancing real-time monitoring of networks. The idea is to use only the papers published from 2024 to 2025 to achieve the aim.

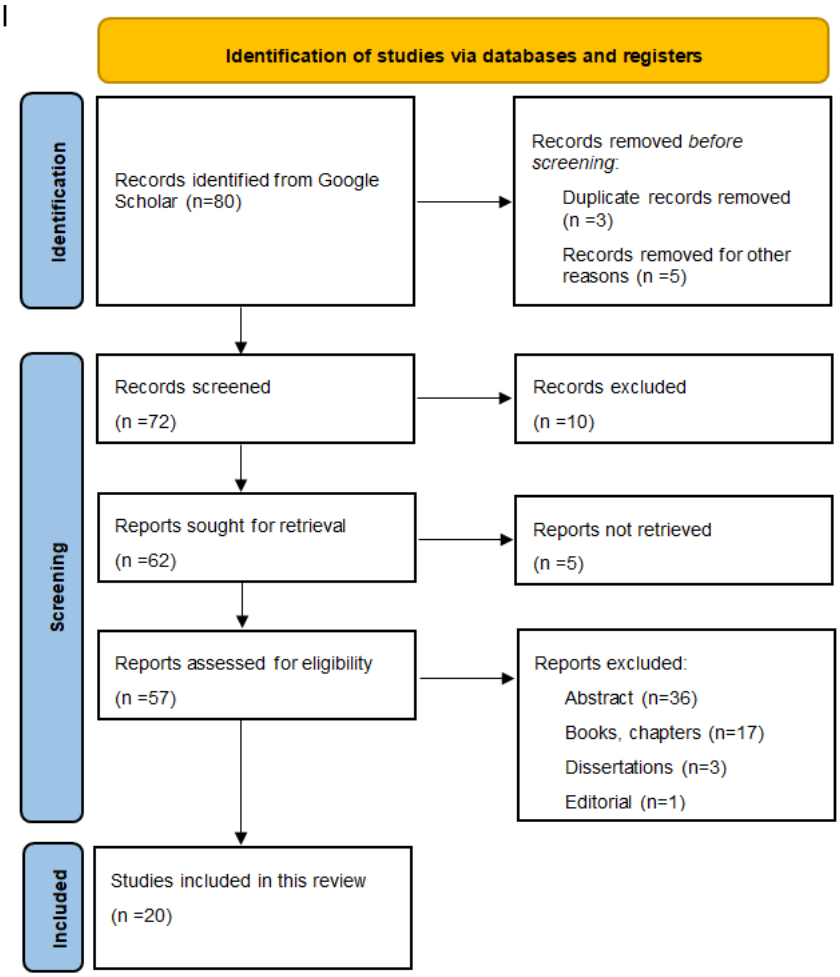
The review is organised as follows: After this Introduction section, the methodology followed to identify, screen and select the papers is described in detail. Then, in the Results section, the selected papers are described. The results obtained by a thematic analysis of the reviewed papers are discussed in the next section. This is followed by Conclusions, Limitations of this review and scope for future research.

METHODOLOGY

For this review, Google Scholar is used for searching and identifying papers. Google Scholar allows selection of papers with a much lower rejection percentage and covers most papers available in databases.

To identify papers, search terms related to the review topic in various combinations were used. This allowed the identification of many papers. The identified papers were screened using some inclusion and exclusion criteria (Table 1) and then a 20 targeted papers were selected. This targeting was done to stress only important points, considering the length of paper allowed by most journals.

The PRISMA flow process was used for screening and selection of papers. The PRISMA flow diagram related to this review is presented below.



Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1

Inclusion and exclusion criteria for this review

Inclusion criteria	Exclusion criteria	Comments
Published in 2024 and 2025 only	Earlier years	To ensure reviewing the latest trends.
Papers in English only	Published in other languages	Even the best translation can distort information.
Only full-text papers	Abstracts	All required details may not be available in abstracts.
Research papers and reviews only	Dissertations, Books, Book chapters, Editorials, Comments, etc.	Research papers and reviews are only helpful in providing the latest trends. Dissertations are supervised information which may be biased in many ways.
	Papers without reference details.	Citation difficulties.

Thematic analysis of the selected papers was done using the procedure prescribed by (Braun & Clarke, 2012). Briefly, the procedure consists of repeated reading to identify themes and subthemes using different colour codes and tabulating the results with the references for each theme-subtheme combination. The tabulated results are presented in this paper.

Besides all the above, the quality of the papers will be assessed as follows:

1. Whether the aim/research questions are provided appropriately based on the research gaps to be addressed?
2. Whether the method used could achieve the aim or answer the research questions fully?
3. Whether the findings match the aim/research questions and method, and address the intended research gaps?
4. Whether the limitations are acknowledged or if not acknowledged, is it possible to identify them independently?

Depending on the levels of agreement with the above points, the overall quality of the paper was rated as 1-Poor, 2-Satisfactory, 3-Good, 4-Fair and 5-Excellent.

An Excel spreadsheet was used to provide the relevant analytical details.

Now, in the results section, the 20 selected papers are described in detail.

RESULTS

Use of cloud computing in businesses is threatened by cybersecurity issues. This is because the traditional intrusion detection systems (IDS) struggle with adapting to the dynamic and complex nature of cloud environments, resulting in flaws and bugs in threat detection and response. To address this issue, Khan (2024) developed an AI-IDS. It uses machine learning algorithms to strengthen cybersecurity in the cloud environment through an in-depth analysis of network traffic trends. Any unusual behaviour in the network traffic pattern may be indicative of cyberattacks. The techniques of unsupervised learning emphasise the use of autoencoders, which enhance the precision of anomaly detection in cloud infrastructure. The authors aimed to demonstrate the effectiveness of the developed AI-IDS system in preventing and protecting cloud devices from cyberattacks. Evaluation of the system showed the benefits of using auto coders for efficient and effective cyber protection systems. Apart from the limitation of not providing the information on the horizontal and

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

vertical axes of the graphs, the model displays a high percentage of false positives. Validation difficulties of abnormal results are also another limitation of the system.

After discussing the basic aspects of security threats and AI solutions, Manda (2024) presented three cases of AT&T, Vodafone and Telefonica from the telecom sector. AT&T has utilised machine learning algorithms to examine network traffic patterns in real-time. By using AI technologies, AT&T can automatically recognise deviations from standard behaviour, such as unexpected surges in data traffic or dubious login attempts. This ability has enabled them to identify and address threats more effectively, which has shortened the average time taken to discover and contain potential security breaches. Vodafone has adopted a threat intelligence platform powered by AI to improve its cybersecurity measures. Utilising advanced analytics, Vodafone can collect and examine data from various sources, such as network devices, customer interactions, and external threat intelligence feeds. This comprehensive strategy allows the company to not only identify threats as they occur but also anticipate potential vulnerabilities by analysing historical data. Consequently, Vodafone has experienced a notable reduction in the number of successful attacks, demonstrating the effectiveness of AI in enhancing security within the telecom sector. Telefonica has implemented AI technologies for identifying threats and managing incidents. Their system utilises natural language processing (NLP) to examine large volumes of data, including social media posts and dark web information, for possible threats. This cutting-edge method enables Telefonica to anticipate emerging risks, offering essential insights that guide their security strategies. By incorporating AI into its security operations, Telefonica has enhanced its capacity to swiftly identify threats, resulting in quicker decision-making and response times.

Goswami (2024) detailed the approach to create and implement an AI-IDS. This involves data acquisition, preprocessing, choosing feature engineering methods, selecting a model for training, integrating ensemble learning, performing real-time monitoring and adaptive measures, as well as evaluating and validating before implementing it into the existing network security framework to align with current security tools, protocols, and processes while ensuring maintenance, ongoing monitoring, and actions are in place. When comparing AI-IDS with other methods and solutions, several important factors should be considered. These include detection accuracy, scalability, adaptability to emerging threats, rates of false positives and false negatives, response time, resilience against evasion techniques, cost-effectiveness, user-friendliness, ease of management, regulatory adherence, and data protection. Although AI-IDS presents numerous potential advantages, it also faces several challenges. These challenges include reliance on data, the risk of overfitting, vulnerability to adversarial attacks, difficulty in model interpretability, high resource requirements, the need for continuous maintenance and updates, ethical and legal concerns, and potential single points of failure. The authors have only discussed the challenges posed by the system without providing examples of the steps involved in developing the AI-IDS.

Vikram, Shnain, Vennila, Sahu, and Krishnakumar (2024) aimed at analysing and outlining an AI-IDS design and comparing it with other models to improve the current network protection. The method involved the use of signature and anomaly detection techniques in parallel, and the use of the ensemble technique for increasing the detector's capabilities and decreasing the false positive rates. The study employed open datasets for training and benchmarking and established that deep learning models, including CNNs and RNNs, can elicit improved results compared to more conventional machine learning models. The authors provided a diagram depicting the steps involved in designing an AI-IDS. The results showed that the ensemble learning model outperformed the models based on decision tree, random forest, SVM, CNN, RNN algorithms and a hybrid approach. The accuracy, precision, recall, F1 score and AUC-ROC were 98.0%, 97.4%, 97.2%, 97.3% and 0.98, respectively, for ensemble learning. These values for others ranged from 93.5% to 97.3%, 96.5% to 92%, 91.5% to 96.3%, 91.8% to 96.4% and 0.92 to 0.97, respectively. The hybrid approach was the second best with values of 97.3%, 96.5%, 96.3%, 96.4%, 0.97, respectively. RNN and CNN performed almost equally.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

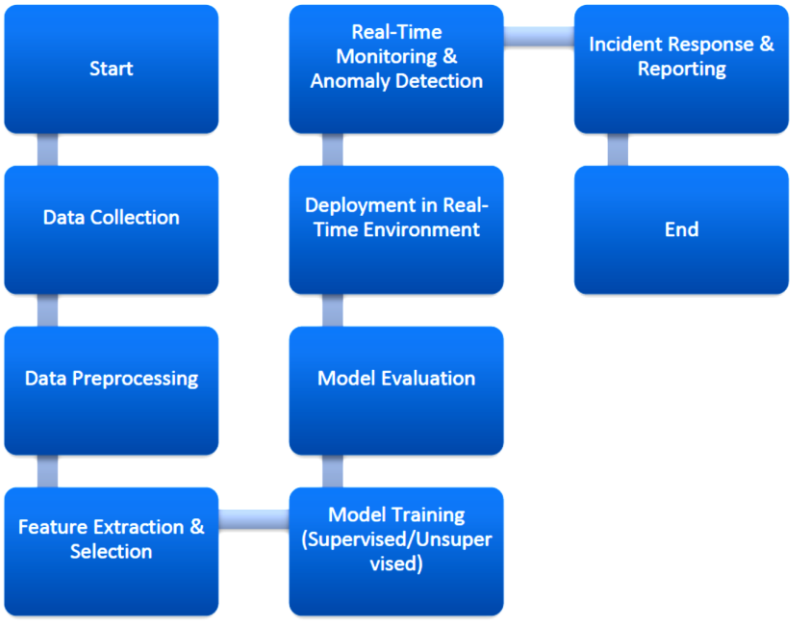
Research Article

The lowest values were reported for the decision tree algorithm. No limitation has been mentioned by the authors.

After discussing ML and DL applications, adaptability, scalability and challenges, Raja (2025) presented case studies involving the integration of Nvidia Morpheus and Generative Adversarial Networks (GANs) to show how the network intrusion detection efficiency of AI-IDS can be enhanced. Also, the performance metrics of a typical AI-IDS were tabulated. Accordingly, the percentage detection in the traditional method was 84.5%, which was improved to 96.8% in the AI-IDS system. False positive rates were 12.7% and 3.2%, respectively. The scalability in terms of network nodes was 1000 and 10000+, respectively. The average response time (secs) was 120 for AI-IDS compared to 450 for the traditional method. No limitation was mentioned. The workflow of AI-IDS is shown in Fig.1. As the diagram shows, the workflow involves data collection, data preprocessing, feature extraction and selection, real-time monitoring, anomaly detection, deployment in a real-time environment, model evaluation, supervised/unsupervised model training and incident response and reporting. The architecture of AI-IDS is presented in Fig.2.

Figure 1

The workflow of AI-IDS (Raja, 2025)



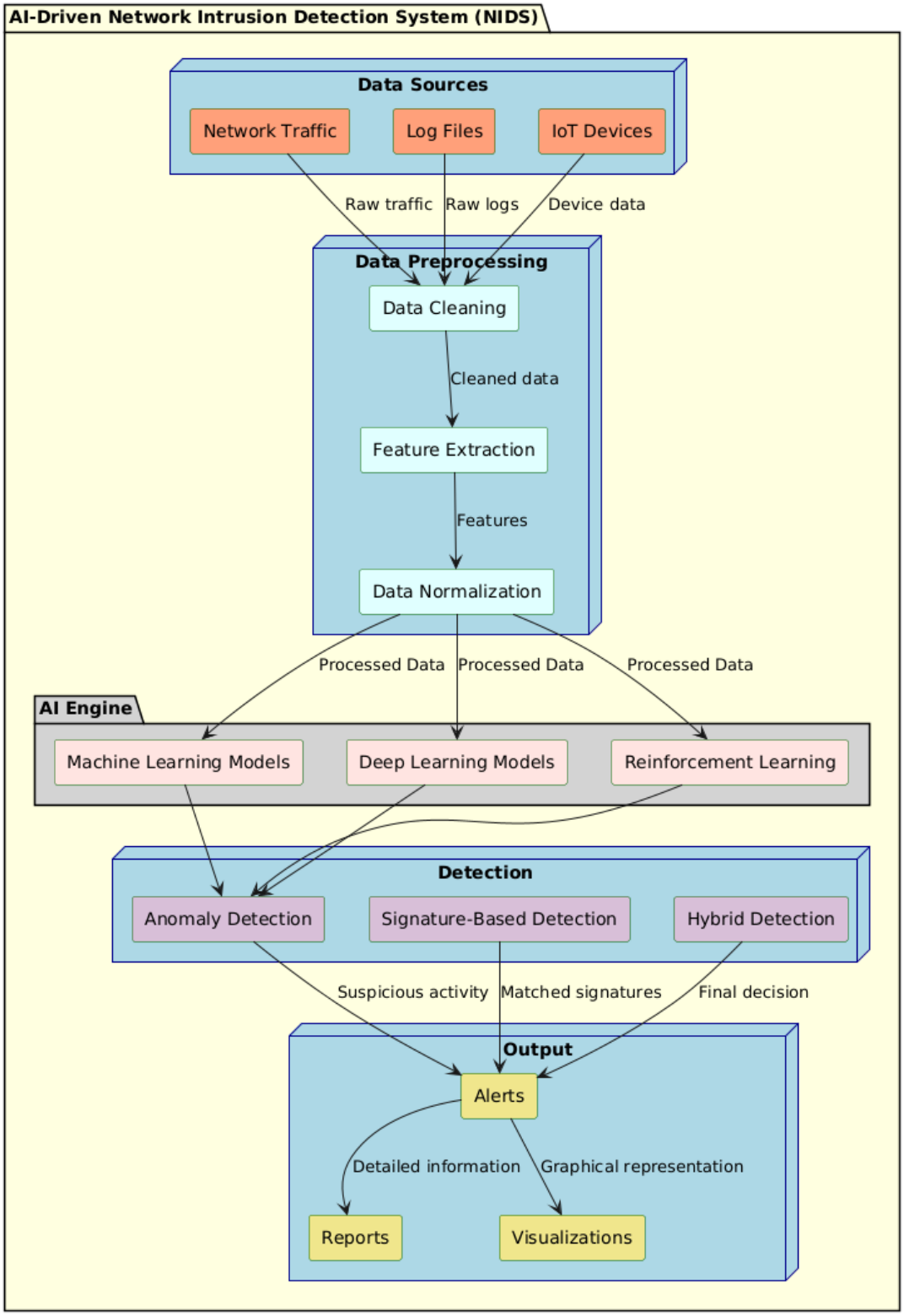
In Fig. 2, the above workflow has been given in more detail. Data sources have been categorised into network traffic, log files and IoT devices. Data preprocessing involves data cleaning, feature extraction and data normalisation. Detection can be based on anomalies, signature-based, or hybrid methods. Output can be in the form of alerts, reports or visualisations. Response as an output is not considered here.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 2

The architecture of AI-IDS (Raja, 2025)



Rai, Rashidov Akbar Ergash o'g'li, Ugli, and Shokirovich (2025) noted that the adoption of AI, including ML and DL, has changed the Network Intrusion Detection Systems (NIDS). AI-powered

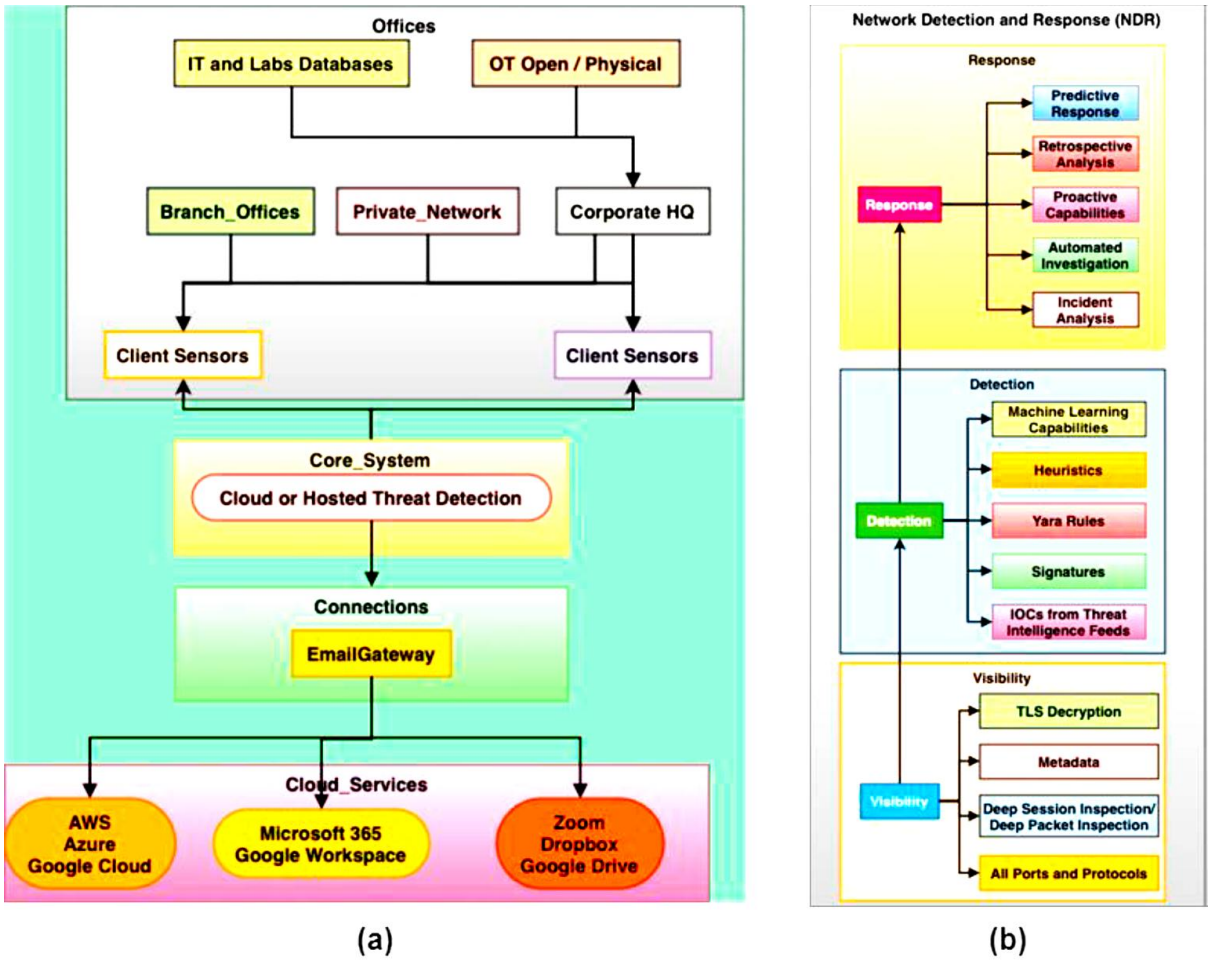
Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

autonomous systems are at the forefront of cybersecurity, excelling in threat detection and protection amid the ever-evolving landscape of cyber threats. Significant advancements have been made in improving detection accuracy and efficiency, establishing a robust cybersecurity framework. The synergy of machine learning and deep learning has enabled the development of more proactive and adaptive mechanisms that continuously evolve to counter emerging threats. Furthermore, the integration of multiple classifiers and blended techniques has fortified NIDS, reducing its vulnerability to specific threats. However, challenges persist, including adversarial attacks, the interpretability of deep-learning models, and the need for lifelong learning. The continuous refinement and enhancement of AI-NIDS remain crucial, emphasising the importance of ongoing research and innovation in cybersecurity. As cyber threats grow increasingly sophisticated, NIDS stands as a vital defence mechanism for organisational security. Looking ahead, the future of cybersecurity is poised for an evolution driven by highly intelligent and adaptable AI-based NIDS, ensuring the protection and integrity of critical digital infrastructures. No limitation is mentioned. The authors have provided an AI-IDS diagram along with a schema of basic NDR.

Figure 3

AI-IDS diagram along with a schema of basic NDR (Rai, Rashidov Akbar Ergash o'g'li, Ugli, & Shokirovich, 2025)



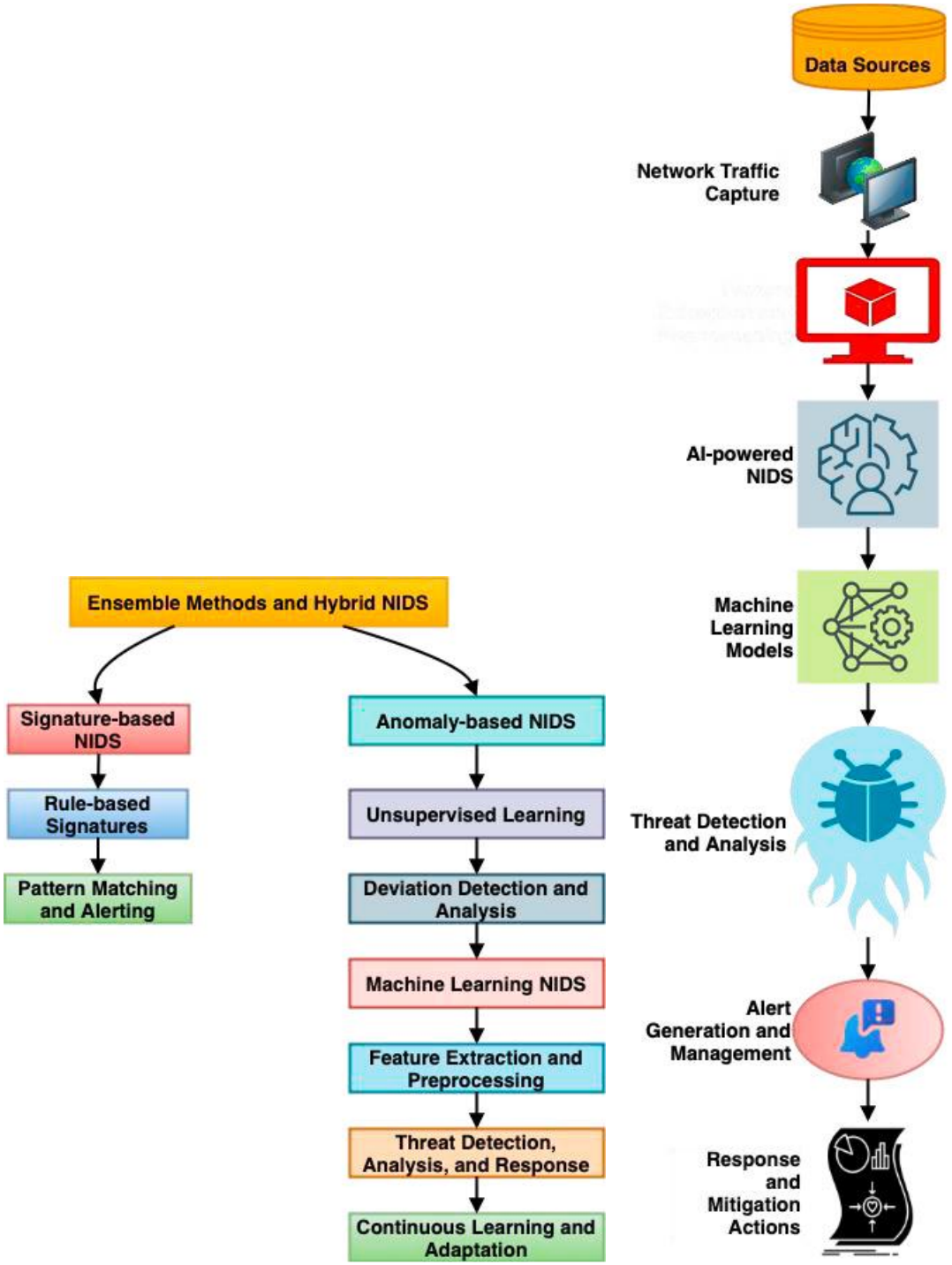
A block diagram of (a) Ensemble methods and hybrid approaches in Network Intrusion Detection Systems (NIDS) (b) Workflow of an AI-IDS has been given in Fig.4.

Figure 4

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A block diagram of (a) Ensemble methods and hybrid approaches in Network Intrusion Detection Systems (NIDS) (b) Workflow of an AI-IDS (Rai, Rashidov Akbar Ergash o'g'li, Ugli, & Shokirovich, 2025)



(a) (b)

The authors discuss the architecture of AI-IDS, the use of ML and DL algorithms in AI-IDS, the transformative impact of AI-IDS, traditional intrusion detection systems, anomaly detection and supervised/unsupervised learning, ensemble and hybrid approaches. After these points, the authors

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

proposed a scheme to enhance cybersecurity systems. In addition to the usual discussion up to threat detection and analysis, the new proposal consists of alert generation and management, a data ingestion layer, ML learning, DL integration and a decision-making module.

Farzaan, Ghanem, El-Hajjar, and Ratnayake (2025) validated an AI-powered cyber incident response system tailored for cloud environments. To assess its effectiveness, the authors tested it against three widely used datasets: NSL-KDD, UNSW-NB15, and CIC-IDS-2017. The Random Forest model demonstrated classification accuracies of 90%, 75%, and 99%, respectively, for network traffic analysis, while achieving 96% precision in malware detection. Additionally, a neural network-based malware analysis model set a new standard with an outstanding 99% accuracy rate. By integrating deep learning models with cloud-based GPUs and TPUs, we showcase how high computational demands can be met without sacrificing efficiency. Moreover, containerization enhances scalability and portability, ensuring seamless deployment across diverse cloud platforms. The system significantly reduces incident response times, mitigates operational risks, and provides cost-effective protection, offering organisations a powerful tool for securing their cloud infrastructure. This pioneering fusion of AI and containerised architecture not only establishes a new benchmark in cyber threat detection but also drives cybersecurity innovation, delivering transformative advantages for critical sectors. The limitations include the absence of a more rigorous validation of the system under different real-world conditions and the challenge of the increasing complexity of anomaly detection.

Muppalaneni, Inaganti, and Ravichandran (2024) developed an AI-driven threat intelligence framework that streamlines data collection, processing, anomaly detection, and automated response to strengthen cybersecurity defences. Leveraging behavioural analysis and pattern recognition, AI models effectively identify cyber threats, reducing manual workload while improving detection accuracy. Adaptive learning techniques, such as reinforcement learning and adversarial training, enable the system to evolve in response to emerging attack strategies. However, the primary drawback is the absence of validation results, limiting assessments of its real-world effectiveness.

For network traffic intrusion detection, Chadrack and Enan (2025) integrated Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) models. It enhanced detection accuracy and operational efficiency. The framework was evaluated using benchmark datasets like UNSW-NB15 and CICIDS2017 on performance metrics. Experimental results showed that the proposed hybrid model achieved a detection accuracy of 92.08%, with precision and recall exceeding 92%, and a low average detection latency of 0.00142 seconds per sample. No limitation mentioned.

Using a review of the literature and case studies on Darktrace, IBM, CrowdStrike, and Microsoft Sentinel, Prince, et al. (2024) observed that the adoption of AI in cybersecurity enhances the protection of information systems through timely identification and prevention of threats. Thus, it maintains high levels of security to prevent data breaches and their impacts. The limitations of the study include the need for a substantial investment in the implementation of AI and the ethical issues in the use of AI. However, AI may not be a perfect solution to cybersecurity challenges, but a critical element of modern data protection systems.

Certainly! Here's a paraphrased version of your text:

Rao, et al. (2024) present an algorithmic framework designed to strengthen IoT network security, comprising five distinct algorithms. The process begins with the Enhanced Anomaly Detection (EAD) algorithm, which identifies anomalies in real-time IoT data, serving as the foundational layer. Building on EAD, the Behaviour Analysis for Profiling (BAP) algorithm incorporates behavioural profiling to enable adaptive detection of abnormal patterns. The Signature-Based Detection (SBD) algorithm leverages pre-defined attack signatures, facilitating the recognition of known threats while providing proactive defence mechanisms. The Machine Learning-Based Intrusion Detection (MLID) algorithm employs trained machine learning models to detect anomalies with dynamic adaptability to evolving security risks. Finally, the Real-Time Threat Intelligence Integration (RTI) algorithm

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

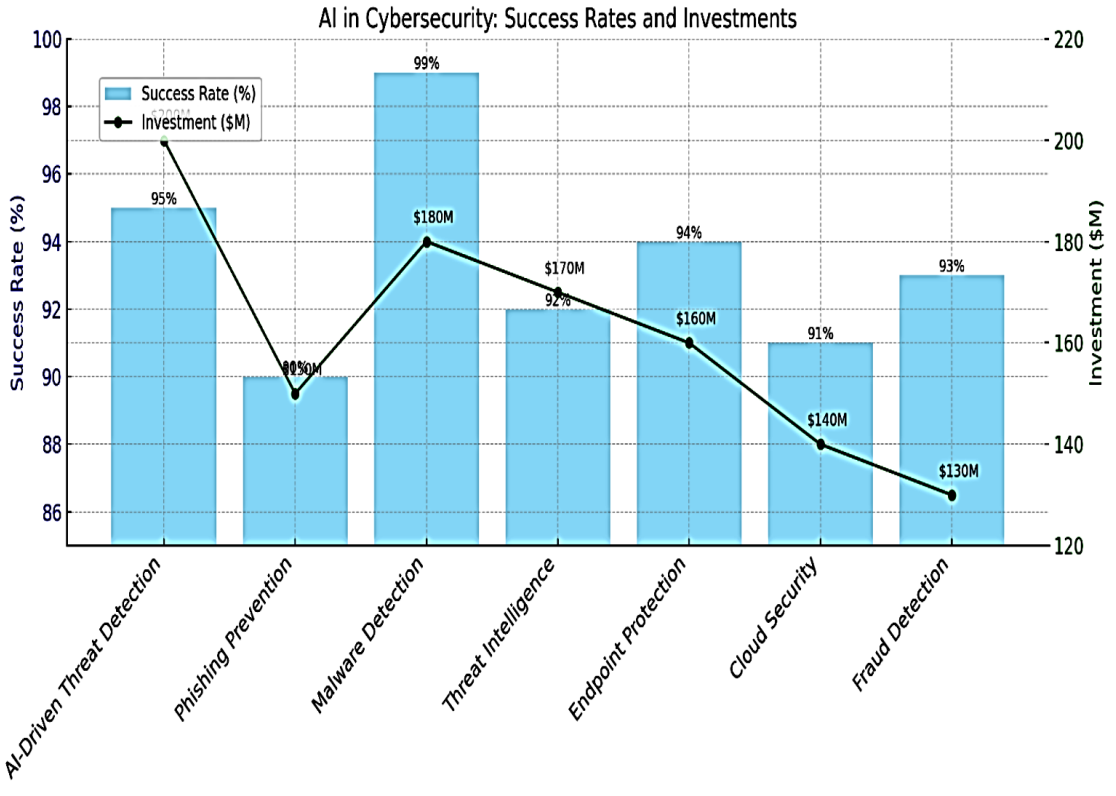
Research Article

enhances the framework's responsiveness by incorporating continuously updated threat intelligence feeds. Visual representations further underscore the framework's precision in integration, applicability, and overall effectiveness in ensuring robust security. A comparison of the proposed EAD algorithm outperformed Behaviour Analysis Profiling, Signature-based Detection, ML-based Intrusion Detection, Real-time Threat Intelligence, Network Segmentation and Isolation, Dynamic Policy Environment, Firmware and Software Patching, User-based Entity Analysis (UBEA) and Incidence Response Automation in terms of accuracy, false positive rate, response time, resource utilisation percentage, scalability and ease of integration. While the proposed EAD recorded 98% accuracy, 1% false positives, 40 ms response time, very high scalability and high ease of integration, the others recorded 88 to 97% accuracy, 1 to 2.5% false positives, 30 to 75 ms response time, moderate to high scalability and moderate to high ease of integration. Regarding accuracy, incident response automation was the next best (97%). No limitation mentioned.

Arjunan (2024) provided a chart of success rates and investments when AI-IDS is used for the detection of cyber threats. This is shown in Fig. 5.

Figure 5

Success rates and investments when using AI-IDS for cyber threat detection (Arjunan, 2024)



As Fig. 5 shows, a generally positive correlation is observed between greater investments and better performance regarding the detection, prevention, and response of threats. No limitation mentioned.

A qualitative review by Singh and Cheema (2024) examined cutting-edge trends and methodologies in AI-driven malware detection systems, with a particular emphasis on their real-time functionality and resilience against adversarial attacks. Through an in-depth evaluation of various algorithms and frameworks, it underscores the advantages of AI, such as enhanced detection accuracy, privacy preservation, and adaptability to evolving malware variants. The findings indicate that traditional signature-based detection approaches have been rendered ineffective by advanced obfuscation methods, whereas AI-powered solutions leverage extensive datasets to identify patterns and

anomalies effectively. Furthermore, the study explores the significance of explainable AI in fostering transparency and interpretability, key factors in establishing user trust and ensuring the reliability of automated security decisions. By synthesising insights from recent research, this review highlights innovative strategies that strengthen detection systems against sophisticated evasion tactics. Ultimately, by mapping the evolving landscape of AI-driven malware detection, this study aims to inform future research directions and contribute to the development of more robust cybersecurity defences capable of countering increasingly sophisticated threats. Some comparative analyses of CNN, RNN and Ensemble models tabulated by the authors show variable results. No limitation mentioned.

In a comprehensive review, Kavitha and Thejas (2024) tabulated various IDS models for their accuracy. The models were DL models, GANs, Explainable AI models, ML ensemble, graph-based learning, transformer models, Federated learning, Domain-adaptive DNNs, Collaborative filtering and Reinforced transformer models. The accuracies of all models ranged between 95% to 100%. Domain-adaptive DNN showed a slight superiority over the others. The accuracy rates reported in the literature varied from 92.3% to 98.2%. No limitation mentioned.

An advanced model proposed by Qureshi, et al. (2025) using AI-powered IDS leveraging Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) networks, using Python and the Kitsune dataset, recorded a detection accuracy of 98.68%, a low False Negative rate of 0.01%, and an F1 score of 98.62%. Comparative analysis with other deep learning models (2D-CNN; DNN; DT, RF, NB; GWO-CNN; KNN-RF-MB, LSTM, MLP; ID-CNN, NB, and RF. LR, SVM) validated the superior performance of our approach. Against an accuracy of 98.66% for the proposed LSTM-GRU model, the accuracy of other models ranged between 86% and 98.59%. Similar comparisons show a precision of 98.44% for the proposed model against the range of 86.65% to 97.25%. The recall percentage for the proposed model was 98.62% against 94.36% to 98% for others. The F1 score for the proposed model was 98.62% against a range of 87% to 98% for others. While the detection time for the proposed model was 6 ms, it was 1100 ms for DT, RF, LR models. No limitation mentioned.

Oloyede (2024) used three case studies of Darktrace, Cisco and Palo Alto to demonstrate the possibility of success in intrusion detection with AI-enhanced systems. These three firms implemented AI-IDS and firewall and AI-powered security platforms. These strategies enhanced their capabilities to detect different types of intrusions into their structures and operations. No limitation mentioned.

Timothy, Rajasekharam, Ampolu, and Mogili (2023) traced the most recent developments in AI-IDS. The authors observed that the AI-driven threat detection systems have undergone significant advancements in accuracy, efficiency, and adaptability. AI-based solutions substantially reduce false positives, enhance detection rates, and enable faster responses to cyber threats compared to traditional rule-based security models. Since AI-driven cybersecurity employs machine learning algorithms that continuously evolve to recognise new threat patterns, it outperforms conventional detection methods. The authors compared DNN, RF, Autoencoder and the traditional rule-based systems. Supervised learning models such as Deep Neural Networks (DNNs) and Random Forest achieved over 95% accuracy and detection rates, while the traditional system achieved only below 80% accuracy and detection rate. in identifying known cyber threats. False positives were less than 2% for DNN compared to 3% or above for other systems. DNN recorded a 40% reduction in response time while other systems recorded 35% or less. For traditional systems, the reduction in response time was less than 10%. No limitation was mentioned.

Mahmud, et al. (2025) employed a mixed-methods approach that combined a systematic literature review with case study analysis. A statistical evaluation was conducted on data from 40 IT initiatives that implemented AI-driven cybersecurity systems. Key performance indicators—such as threat detection time, risk mitigation efficiency, and overall security effectiveness—were assessed both before and after AI integration. The findings indicate a 35% reduction in threat detection time, a 25%

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

improvement in risk mitigation efficacy, and a 45% increase in threat identification accuracy, collectively leading to a substantial decline in cybersecurity breaches. These results underscore the transformative impact of AI on cybersecurity within IT project management. The study concludes that AI-powered cybersecurity models offer a promising approach for proactive risk mitigation and strengthening IT projects' security posture. A comparison of traditional and AI-driven methods showed an accuracy of 68% for traditional and 92% for the AI-driven methods. Mean detection time was 5.3 and 3.2 hrs, respectively. False positive rates were 45% and 25%, respectively. Incidence response time declined from 45 minutes for traditional to 20 minutes for the AI-driven methods. Risk mitigation efficiency was 78% for the AI-driven compared to 60% for traditional methods. The limitations were small sample size and the issue of tools becoming obsolete due to the rapid developments in this area of research.

Kumar, et al. (2025) compared AI-based models based on Random Forest, Support Vector Machines (SVM), Deep Learning, and K-Means Clustering for improved threat detection. The study used a dataset of 500,000 cybersecurity incidents, examining attack patterns, anomaly detection, and fraud prevention systems. Deep Learning model recorded maximum accuracy at 96.8%, surpassing SVM at 92.3% and Random Forest at 94.1% for the detection of ransomware and intrusion attempts. K-Means Clustering also successfully classified malicious behaviour at a detection level of 89.5%. The findings indicate that AI-driven techniques significantly enhance real-time cyber threat mitigation compared to traditional methods. Additionally, integrating blockchain and big data analytics improves financial transaction fraud detection by 35%, reducing false positives. The research concludes that AI and machine learning offer superior accuracy, adaptability, and speed in cybersecurity applications. However, challenges such as computational costs and adversarial attacks require further optimisation. Future studies should focus on developing more interpretable and scalable AI models to strengthen global cybersecurity resilience. No limitation mentioned.

Gujar (2024) presented an ML-integrated intrusion detection system (IDS) that leverages advanced machine learning techniques—including neural networks, support vector machines, and reinforcement learning—to improve identification accuracy, minimise false alarms, and reduce detection delays. The evaluated research, conducted within a simulated critical infrastructure environment and tested using the NSL-KDD dataset, demonstrated notable performance metrics: a detection accuracy of 95%, a false positive rate of 4%, and an average detection latency of 0.8 seconds. The system exhibited enhanced flexibility and efficiency in threat detection and response, delivering superior real-time performance. These advancements over traditional methods highlight the considerable potential of AI-driven IDS in strengthening the protection of critical assets against emerging and sophisticated cyber threats. However, no data on the traditional system has been given for comparison. The author has not mentioned any limitations.

DISCUSSION & CONCLUSION

Thematic analysis

The results of thematic analysis are presented in Table 2.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 2

Thematic analysis of the reviewed papers

Theme	Subtheme	References	Frequency	
Aim	Demonstrate/validate a newly developed AI-IDS system	1, 7, 11, 15, 20	5	
	To illustrate AI-powered platforms transforming threat intelligence into a proactive, dynamic function	2	1	
	To describe the methods and challenges of developing and implementing an AI-IDS.	3	1	
	Compare with other models/systems	4, 6, 17, 18, 19	5	
	General discussions on AI-IDS	5, 8, 10,12, 13, 14,16	7	
	To intevgrate two systems	9	1	20
Method	Developing and evaluation	1	1	
	Case studes	2, 10,16	3	
	Discussion	3, 5, 6,8	4	
	Compare with other models/systems	4, 7,11,14, 15, 18, 19, 20	8	
	Experiment	9	1	
	Literature survey	12, 13, 17	3	20
Findings	Positive for AI-IDS	All positive.		20
Limitations	Some required information absent	1,20	2	
	High false positives rate	1	1	
	Anomaly detection problems	1	1	
	NA	2, 4,5,6, 7, 11, 12, 13, 14, 15, 16, 17, 19, 20	14	
	Challenges of the system	3	1	
	Inadequate rigour in testing	7	1	
	Validation inadequacies	8	1	
	Higfh investments to implement the model	9	1	
	Small sample size	18	1	23*
	*Some papers had more than one limitation.			

As could be seen from Table 2, general discussions predominated among the aims with 7 out of 20 papers using this as the aim. Seeing too many general discussions, this reviewer selected papers which report empirical findings, including model validation and comparisons of models. Together they accounted for 10 papers. Three aims had only a single paper.

Among methods, comparisons with models accounted for 8 out of 20 papers. There were four discussion papers. The number of discussion papers in the aim and the method does not match because three papers dealt with comparisons with data.

Not surprisingly, all findings favoured AI-IDS with positive results. Only the challenges made it difficult to implement it in all contexts.

Out of 20 papers, 14 did not mention any limitation (NA in the table). All other limitations were reported by only one paper each. The total number is more than 20 since three papers reported more than one category of limitations.

Quality of the reviewed papers

Table 3 gives the quality trends of the reviewed papers. The method used to assess the quality of the papers is described in the Methodology section. The scores were converted to ranges to produce frequencies as shown in Table 3.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 3

Quality of the reviewed papers

Score range	Frequency
8 to 11	6
12 to 15	10
16 to 19	4

It can be seen that the general trend is an attempt to shift from low to medium quality. The large number of discussion papers repeating the same points lowered the quality of the reviewed papers. Notably, four papers were of the highest quality. The maximum rating of 19 was scored by the paper by Mahmud et al.(2025). The minimum rating of 8 was scored by Singh & Cheema (2024).

LIMITATIONS OF THIS REVIEW

Many important papers might have been missed due to the use of Google Scholar only for identifying the papers and setting a target of 20 papers. The trends of thematic analysis and quality of the papers should be accepted with caution as they are based on 20 papers only. A large number of papers might have shown different trends. Many papers only discussing the AI-IDS and not providing limitations have also affected the quality of this review.

SCOPE FOR FUTURE RESEARCH

As is clear from the above discussion, more higher quality papers reporting empirical results and using mixed methods are required. Methods to mitigate the shortcomings of AI-IDS need to be researched further. Integration of AI-IDS with the current detection systems needs to be researched further. Most papers provide only intrusion detection methods. There is an urgent need to evolve predictive models, which can help proactive prevention of intrusions and methods for damage control when a serious intrusion has occurred.

CONCLUSIONS

There is no doubt about the superiority of AI-based intrusion detection systems. Only the components of such systems differ depending on the target of the detection system, like cloud computing, IoT or internal structures and operating systems. The challenges to the implementation of AI-based intrusion detection systems in organisations have been identified. Solutions to these have been suggested. However, it is not known whether any of these solutions have been implemented successfully by any organisations is unknown. Some case studies on big and small organisations can enlighten us on this aspect.

REFERENCES

[1] Arjunan, G. (2024). AI-Powered Cybersecurity: Detecting and Preventing Modern Threat. *International Journal of Innovative Science and Research Technology, 9*(11), 1949-1955. Retrieved May 24, 2025, from https://www.researchgate.net/profile/Gopalakrishnan-Arjunan/publication/387897172_AI-Powered_Cybersecurity_Detecting_and_Preventing_Modern_Threat/links/67820749a1cf464e7d272ae7/AI-Powered-Cybersecurity-Detecting-and-Preventing-Modern-Threat.pdf

[2] Braun, V., & Clarke, V. (2012). *Thematic analysis: A Practical Guide*. Sage Publications. Retrieved October 5, 2024, from https://www.google.co.in/books/edition/Thematic_Analysis/mToqEAAAQBAJ?hl=en&gbpv=0

[3] Chadrack, I., & Enan, N. M. (2025). AI Powered Network Traffic Detection. *Journal of Information and Technology, 5*(2), 53-65. Retrieved May 24, 2025, from

https://edinburgjournals.org/journals/index.php/journal-of-information-technolog/article/view/464

[4] Farzaan, M. A., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2025). AI-powered system for an efficient and effective cyber incidents detection and response in cloud environments. *IEEE Transactions on Machine Learning in Communications and Networking, 3*, 623-643. doi:https://doi.org/10.1109/TMLCN.2025.3564912

[5] Goswami, M. (2024). Enhancing Network Security with AI-Driven Intrusion Detection Systems. *International Journal of Open Publication and Exploration, 12*(1), 29-36. Retrieved May 23, 2025, from https://www.researchgate.net/profile/Maloy-Jyoti-Goswami-2/publication/381280612_Enhancing_Network_Security_with_AI-Driven_Intrusion_Detection_Systems/links/6664d39db769e76919252270/Enhancing-Network-Security-with-AI-Driven-Intrusion-Detection-Systems.pdf

[6] Gujar, S. S. (2024). AI-Enhanced Intrusion Detection Systems for Strengthening Critical Infrastructure Security. *Global Conference on Communications and Information Technologies (GCCIT), 25-26 October 2024, Bengaluru, India* (pp. 1-7). IEEE. doi:https://doi.org/10.1109/GCCIT63234.2024.10861950

[7] Kavitha, D., & Thejas, S. (2024). AI-enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE Access, 12*, 173127-173136. doi:https://doi.org/10.1109/ACCESS.2024.3493957

[8] Khan, M. M. (2024). Developing AI-powered intrusion detection system for cloud infrastructure. *Journal of Artificial Intelligence, Machine Learning and Data Science, 2*(1), 1074-1080. doi:https://doi.org/10.51219/JAIMLD/mohammed-mustafa-khan/255

[9] Kumar, B. H., Nuka, S. T., Malempati, M., Sriram, H. K., Mashetty, S., & Kannan, S. (2025). Big Data in Cybersecurity: Enhancing Threat Detection with AI and ML. *Metallurgical and Materials Engineering, 31*(3), 12-20. doi:https://doi.org/10.63278/1315

[10] Mahmud, F., Barikdar, C. R., Hassan, J., Goffer, M. A., Das, N., Orthi, S. M., . . . Hasan, R. (2025). AI-Driven Cybersecurity in IT Project Management: Enhancing Threat Detection and Risk Mitigation. *Journal of Posthumanism, 5*(4), 23-44. doi:https://doi.org/10.63332/joph.v5i4.974

[11] Manda, J. K. (2024). AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations. *International Journal of Multidisciplinary and Current Educational Research, 6*(2), 333-340. doi:https://dx.doi.org/10.2139/ssrn.5003638

[12] Muppalaneni, R., Inaganti, A. C., & Ravichandran, N. (2024). AI-Driven Threat Intelligence: Enhancing Cyber Defense with Machine Learning. *Journal of Computing Innovations and Applications, 2*(1), 1-11. doi:https://doi.org/10.63575/

[13] Oloyede, J. (2024). *Leveraging Artificial Intelligence for Advanced Cybersecurity Threat Detection and Prevention*. SSRN. doi:https://dx.doi.org/10.2139/ssrn.4976072

[14] Prince, N. U., Faheem, M. A., Khan, O. U., Hossain, K., Alkhayyat, A., Hamdache, A., & Elmouki, I. (2024). AI-powered data-driven cybersecurity techniques: Boosting threat identification and reaction. *Nanotechnology Perceptions, 20*(S10), 332-353. Retrieved May 24, 2025, from https://www.researchgate.net/profile/Muhammad-Ashraf-Faheem/publication/384441701_AI-Powered_Data-Driven_Cybersecurity_Techniques_Boosting_Threat_Identification_and_Reaction/links/66f9408a9e6e82486ff584e0/AI-Powered-Data-Driven-Cybersecurity-Techniques-Bo

[15] Qureshi, S. S., He, J., Qureshi, S. U., Zhu, N., Wajahat, A., Nazir, A., . . . Wadud, A. (2025). Advanced AI-driven intrusion detection for securing cloud-based industrial IoT. *Egyptian Informatics Journal, 30*, 100644. doi:https://doi.org/10.1016/j.eij.2025.100644

[16] Rai, H. M., Rashidov Akbar Ergash o'g'li, A. P., Ugli, B. A., & Shokirovich, Y. S. (2025). Advanced AI-Powered Intrusion Detection Systems in Cybersecurity Protocols for Network Protection. *Procedia Computer Science, 259*, 140-149. doi:https://doi.org/10.1016/j.procs.2025.03.315

[17] Raja, M. S. (2025). The Rise of AI-Driven Network Intrusion Detection Systems: Innovations, Challenges, and Future Directions. *International Journal of AI, BigData, Computational and Management Studies,, 6*(1), 1-9. doi:https://doi.org/10.63282/3050-9416.IJAIBDCMS-V6I1P101

[18] Rao, D. D., Waoo, A. A., Singh, M. P., Pareek, P. K., Kamal, S., & Pandit, S. V. (2024). Strategizing IoT network layer security through advanced intrusion detection systems and AI-driven threat analysis. *Journal of Intelligent Systems and Internet of Things, 12*(2), 195-207. doi:https://doi.org/10.54216/JISIoT.120215

[19] Singh, B., & Cheema, S. S. (2024). Emerging Trends in AI-Powered Malware Detection: A Review of Real-Time and Adversarially Resilient Techniques. *Tuijin Jishu, 45*(4), 1841-1869. Retrieved May 24, 2025, from https://www.researchgate.net/profile/Bhagwant-Singh-4/publication/388405244_Emerging_Trends_in_AI-Powered_Malware_Detection_A_Review_of_Real-Time_and_Adversarially_Resilient_Techniques/links/6797270b4c479b26c9baaa3c/Emerging-Trends-in-AI-Powered-Malware-D

[20] Timothy, M. J., Rajasekharam, B., Ampolu, K. V., & Mogili, U. (2023). Threat Detection Using AI in Cybersecurity Systems. *International Journal of Innovation Studies, 7*(1), 1-8. Retrieved May 24, 2025, from https://www.researchgate.net/profile/Umamaheswara-Mogili/publication/388709430_Threat_Detection_Using_AI_in_Cybersecurity_Systems/links/67a357278311ce680c537d4d/Threat-Detection-Using-AI-in-Cybersecurity-Systems.pdf#page=4.82

[21] Vikram, A., Shnain, A. H., Vennila, R. J., Sahu, P., & Krishnakumar, K. (2024). AI-Powered Network Intrusion Detection Systems. *IEEE International Conference on Communication, Computing and Signal Processing (IICCCS), 19-20 September 2024, Asansol, India* (pp. 1-6). IEEE. doi:https://doi.org/10.1109/IICCCS61609.2024.10763627