Communication in Physical Sciences, 2026, 12(8): 2399-2410

Enhancing Cloud Security Using Predictive AI Analysis: A Systematic Review of Literature

Dahunsi Samuel Adeyemi.
Received: 22 November 2025/Accepted: 3 December 2025 /Published: 13 December 2025
https://dx.doi.org/10.4314/cps.v12i8.18

Abstract: *Generally, it has been established that traditional methods of cloud security are plagued with different inadequacies and ineffectiveness. Thus, this study examined how cloud security can be enhanced using predictive AI models. The study adopted the systematic review approach, using the Preferred Items for Systematic Review and Meta-analysis (PRISMA) for data collection. The secondary data were collected from credible databases, which include Google Scholar, Scopus, Taylor and Francis, EBSCOHost, and Emerald, using the appropriate search terms. A total of seventeen (17) articles constitutes the final selected literature. Collected data was analyzed using the "a priori" thematic analysis. The study found that cloud vulnerabilities that are prevalent include detecting anomalies, intrusions, phishing, identify fraud, IoT-enhanced attacks, and malware that compromise infrastructure. Results showed that there are a diverse of predictive AI models used to address these threats include CNNs, Random Forests, SVMs, Naïve Bayes, Decision Trees, LSTMs, BiLSTMs, and Transformers. The findings showed that the predictive AI models used are largely effective in improving cloud security, highlighting how it reduced false positive rates, faster detection speeds, and enhance real-time monitoring performance. Results showed public intrusion datasets such as UNSW-NB15, CIC-IDS2017, and CSE-CIC-IDS2018 are mostly used due to their standardization and structured labelling. Findings showed that there is a heavy reliance on standard classification metrics. Despite all the benefits of AI-enhanced cloud security, challenges such as shortage of high-quality, labelled, and representative datasets affect its effective implementation. The study concludes that predictive AI models enhance cloud security.*

Keywords: *cloud security, cloud computing, predictive AI models, deep learning techniques, cloud vulnerabilities*

Dahunsi Samuel Adeyemi.
Department of Computer Science and Cybersecurity, University of Central Missouri Missouri, USA. College of Health, Science and Technology.
Email: dxa26930@ucmo.edu
https://orcid.org/0009-0007-5485-8052

1.0 Introduction

Computing technologies have undergone significant transformations over the past decades, culminating in the emergence of cloud computing as a dominant paradigm for data storage, processing, and service delivery. One of these is the idea of cloud computing. Specifically, cloud computing has helped both individuals and organizations to collect, store, process, and access information using scalable computing resources with the aid of the internet facility. Cloud environments provide opportunities to maximize virtualized resources hosted by cloud service providers. Some of the benefits of these virtualized services include flexibility, seamless collaboration, cost efficiency, and so on. All these benefits known, the shared and distributed nature of cloud computing enhances potential attack with its unique security challenges, which differs from the traditional on-premises systems. Some of the challenges include data breaches, account hijacking, unauthorized access, and compliance

requirements, among others. Therefore, cloud security encompasses policies, practices, technologies, and designs implemented to protect cloud-based data, applications, and infrastructure.

Cloud security refers to the collection of policies, technologies, and control mechanisms designed to protect cloud-based data, applications, and infrastructure by ensuring confidentiality, integrity, and availability of resources. (Singh & Chatterjee, 2017). Akinade et al. (2025) noted that cloud security involves a set of practices, technologies, and policies that are designed to protect data, applications, and infrastructure within cloud environments. The authors noted further that providing cloud security includes managing identity and access, encryption, network security, and incident response protocols. All of these highlight that cloud security issues may include unauthorized access, data breaches, and various cyber threats. Zhang et al. (2013) described cloud computing security as a wide range of principles, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Collectively, these studies demonstrate that cloud security threats arise from both technological architecture and operational management complexities, suggesting that conventional perimeter-based security approaches are insufficient for modern cloud ecosystems. For example, Butt et al. (2023) identified information threat, network threat, and cloud condition-specific threats as some of these issues. It was further stated that while cloud condition-specific threats include unreliable interfaces and APIs, dangerous insiders, misuse of cloud administrations, and shared development vulnerabilities, information threats concern data breaches and data loss, while network threats include record or administration hijacking, and service refusal. Meanwhile, the Cloud Security Alliance (CSA) identifies data breaches and data loss as two of the top nine threats in cloud computing, which can arise as a result of the complexity of the cloud scenario such as dynamic distribution, virtualization, and multitenancy (Samarati & De Capitani di Vimercati, 2016). Essentially, information security or data security is what describes cloud security, which may include concern interaction among people, software, and services on the Internet (Tissir et al., 2021). All of these are believed to encapsulate the idea of cybersecurity.

Cloud security is an important part of cloud computing, which addresses risk management, threat analysis, data protection, identity and access management, and compliance (Murthy et al., 2024). Guaranteeing security in the cloud means that some factors are considered in order to ensure robust and reliable protection of data in the cloud. Thus, this will help enhance confidentiality and integrity of data, access to it, and computations with it, as well as ensuring the availability of data and services to legitimate users in compliance with agreements with providers (Samarati & De Capitani di Vimercati, 2016). Birje et al. (2017) indicate that cloud computing system should be based on trust, which makes security and confidentiality a major issue affecting its widespread adoption. Without trust between the service providers and users, there may be challenge with its adoption and/or acceptance. This emphasizes the importance of cloud security in a cloud computing system.

Cloud security is an essential element of safeguarding cloud resources and facilities. However, there are different kinds of cloud issues. Maroc & Zhang (2019) attempted to distinguish cloud-specific security issues from traditional ones based on the characteristics supporting the cloud model, while others categorize issues based on cloud service models, components, or stakeholders' perspectives. Alani (2016) discussed the elements of cybersecurity, distinguishing how cloud security differs from classical systems security. The author provides a comprehensive

list of nine common security threats that embody what is understood to be cyber security. These identified threats include: data breaches, data loss, account or service hijacking, insecure interfaces and APIs, threats to availability, malicious insiders, abuse of cloud services, insufficient due diligence, and shared-technology vulnerabilities.

Despite the development of several conventional cloud security mechanisms, existing approaches remain largely reactive and struggle to address rapidly evolving and intelligent cyber threats. Thus, there is a need to improve the traditional systems using other methods or approaches. Parisa and Banerjee (2024) established that AI-driven cybersecurity models significantly outperformed traditional security mechanisms in terms of threat detection accuracy, false positive rates, response time, scalability, and adaptability to emerging cyber threats. Polamarasetti (2024) noted that AI-powered authentication and access control systems enhance identity management, which helps curb the issues of data breaches and unauthorized access. This buttresses the notion that AI-enhanced systems would identify trends, outliers, and potential dangers from large datasets that it has been trained with. Stutz et al. (2024) established that AI-centered cloud computing security is effective to hinder unauthorized access and numerous cyber-attacks or threats.

AI-enhanced cloud computing security can take different models and/or learning approaches to boost security architecture or design. Different studies (e.g. Kumari, 2022; Vashishth et al., 2024) have emphasized the importance of Artificial Intelligence (AI) and Machine Learning (ML) in improving cloud security. For instance, Attou et al. (2023) recommended the use of Machine Learning (ML) and Deep Learning (DL) approaches to improve Intrusion Detection System (IDS) performance. In a multi-cloud environment, Salman et al. (2017) noted that machine learning techniques such as Linear Regression (LR) and Random Forest (RF) can be used to build intrusion detection systems (IDS), which can be used to detect anomalies in network traffic (an important aspect of cloud security). Additionally, some machine learning techniques, such as Support Vector Machines (SVM), Neural Networks (NN), and Deep Neural Networks (DNN) have been used to monitor cybersecurity threats in cloud environments (Adeyemi, 2024; Sokolov et al., 2019). While these studies demonstrate promising performance improvements, variations in datasets, evaluation metrics, and deployment environments make it difficult to draw generalized conclusions regarding the overall effectiveness of predictive AI in cloud security.

The increasing growth of cloud computing has transformed the operations of different organizations with respect to the storage, management, and access of data (Sunyaev, 2020). This transformation, however, has brought about complex security challenges that the hitherto traditional approaches may not be able to address. More importantly, the incorporation of third-party services in cloud computing opens up the services to the risks of insider threats, misconfigured resources, account hijacking, and advanced persistent attacks (Duncan et al., 2015; Sharma & Sharma, 2024). Meanwhile, predictive artificial intelligence (AI) has been proposed by scholars to have the ability to identify patterns and forecast anomalies in large datasets before security is breached at all (Nwoye & Nwagwughiagwu, 2024). However, existing studies are largely fragmented, focusing on specific algorithms or isolated applications without providing a comprehensive synthesis of predictive AI models, datasets, evaluation metrics, and implementation challenges within cloud security contexts. Nonetheless, evidence remains fragmented with respect to its actual effectiveness, implementation requirements, scalability, algorithm reliability, and ethical

issues. To address these limitations and provide a consolidated understanding of current advancements, this study systematically reviews existing literature on the application of predictive AI analysis for enhancing cloud security. This study is significant in several respects. First, it provides a structured synthesis of predictive AI applications in cloud security, thereby bridging fragmented findings across existing studies. Second, it offers practitioners and cloud service providers evidence-based insights into effective AI-driven security mechanisms capable of improving threat detection and response efficiency. Third, the study identifies methodological and data-related limitations that may guide future research toward developing scalable, reliable, and ethically responsible AI-enabled cloud security frameworks. Accordingly, this study addresses the following research questions:

i. What cloud security threats are most commonly addressed using predictive AI techniques?
ii. Which are the predictive AI models employed to improve cloud security?
iii. What is the effectiveness of the employed AI models in improving cloud security?
iv. What datasets are commonly used in applying AI models to cloud security?
v. What are the evaluation metrics for AI models used for cloud security?
vi. What are the challenges associated with the application of predictive AI models for cloud security?

2.0 Methodology

This study adopts a systematic literature review (SLR) methodology to examine how cloud security can be enhanced using predictive artificial intelligence (AI) analysis. The systematic review methodology provides a structured, transparent, and replicable process for synthesizing existing evidence, thereby improving methodological rigor compared with traditional narrative reviews (Adeyemi et al., 2025). The systematic review approach was selected because it minimizes researcher bias, enhances reproducibility, and follows established procedural guidelines that support empirical evidence synthesis. Schut et al. (2024) noted that the approach requires searching academic databases for relevant literature in the area of study. The authors recommended seeking literature from reliable academic databases to ensure that the evidence would be credible. For this reason, five (5) academic databases were consulted for the literature search in this study. These databases include Google Scholar, Scopus, Taylor and Francis, EBSCOHost, and Emerald. These databases were selected due to their extensive coverage of peer-reviewed publications in computer science, information systems, and cybersecurity research.

A structured keyword-based search strategy was employed to retrieve studies relevant to the research questions. In the literature search, relevant keywords and search terms can help enhance the return rate of literature that would answer the identified research questions in this study. The Sample, Phenomenon of Interest, Design Evaluation, and Research Type (SPIDER) was used as a search strategy to consult the five (5) academic databases. The Sample, Phenomenon of Interest, Design, Evaluation, and Research Type (SPIDER) framework (Table 1) was adopted to structure the search strategy because it accommodates qualitative, quantitative, and mixed-methods studies. Also, it allows for the use of a mixed-methods research approach (Amir-Behghadami & Sadeghi-Bazarghani, 2021). This allowed for having a wide-ranging resources and evidence with respect to the use of predictive AI analysis to enhance cloud security. Boolean operators ("AND" and "OR") were applied to refine and expand search combinations across databases, thereby improving retrieval sensitivity (Schut et al.,

2024). The operator "NOT" was excluded to avoid unnecessary loss of potentially relevant studies.

Table 1: SPIDER Tool

SPIDER	Content
Sample	Cloud service providers, organization users, cloud computing environments
Phenomenon of Interest	Use of predictive AI models and algorithm
Design	Published literature of both qualitative and quantitative approaches
Evaluation	The effectiveness of predictive AI models for cloud security
Research type	Qualitative and quantitative research

Source: Author's fieldwork (2025)

Application of the SPIDER framework enabled a systematic identification of studies examining predictive AI applications in cloud security. Using the SPIDER tool, a large number of hits were returned from the five (5) academic databases that were consulted. Consequently, inclusion and exclusion criteria were introduced, which evaluate the search results to produce only the most relevant literature for this systematic review (see Table 2). Explicit inclusion and exclusion criteria were defined to ensure relevance, methodological quality, and alignment with the study objectives. The criteria in this study include the year range, which is left at fifteen (10) publication period restricted to a ten-year range (2015–2025), years range [2015-2025], removal of duplicated publications, removal of literature published in other languages aside from English, primary research, studies conducted in the area of cloud computing security, full-text articles, and mixed-methods research approach. Using these criteria, the final selected literature is seventeen (17) articles.

Table 2: Inclusion and Exclusion Criteria

Inclusion and exclusion criteria	No. of hits	Justifications for search criteria
Studies published between the years 2015-2025	538	This is to ensure that only recent evidences are used in the answering the research question.
Duplicate publications removed	412	This is to avoid redundancy in the retrieved literature
Literature published in the English language	384	This is to ensure that all the literature are in an understandable language to allow analysis
Primary research only	216	This is to have only original primary research findings with respect to the research
Studies published in the area of cloud computing security	140	This is to contextualize the literature analysis to studies that were conducted in the area of cloud security
Full-text only	48	Full-text allows critical review and analysis of the literature

Qualitative or quantitative research only	17	This is to analyze research findings that provide deeper understanding of experience, phenomenon, and context

Source: Author's fieldwork (2025)

Meanwhile, the data collection process was ensured in a similar structured manner through Preferred Reporting Items for Systematic Review and Meta-analyses (PRISMA) (see Fig. 1). The framework is appropriate for systematic review studies, which is one this study adopted. Meanwhile, the framework has four (4) phases, which include identification, screening, eligibility, and inclusion. In the initial search of the different databases, a total of 538 items were extracted from the different databases.

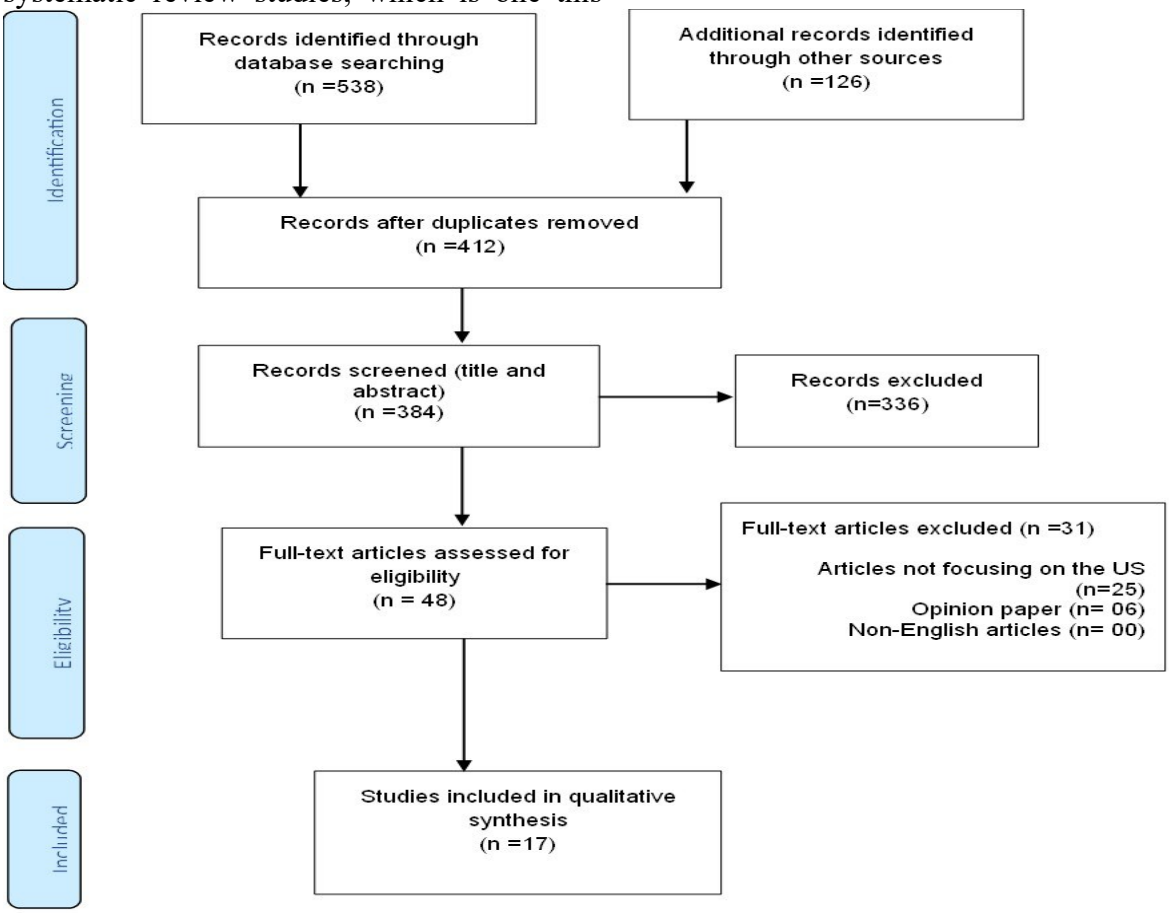

Fig. 1. PRISMA Flow Diagram Illustrating the Study Selection Process for the Systematic Review

Source: Author's Fieldwork (2025)

After this, duplications were checked and only four hundred and twelve (412) items from the collected data were expunged as having duplicates in the returns. Next, the titles and abstracts of the articles were checked for relevance and whether they are relatable to the current study, and only twenty-eight (28) articles were removed. After all these, the remaining items were examined with the inclusion and exclusion criteria that were set for the study. From this, only fifteen (17) articles were finally selected for this study.

These seventeen (17) studies constituted the analytical dataset for the review. Relevant information from each selected study was systematically extracted using a standardized data extraction form (Appendix I), including study objectives, AI models, datasets, evaluation metrics, and key findings. Data were analyzed using an a priori thematic analysis approach, whereby predefined analytical themes derived from the research questions guided coding and synthesis of findings.

Data were analyzed using an a priori thematic analysis approach, whereby predefined analytical themes derived from the research questions guided coding and synthesis of findings.

3.0 Results and Discussion

With respect to Research Question 1, the findings reveal a recurring concentration of dominant cloud security threats addressed by predictive AI models. The recurring theme shows a strong emphasis on detecting anomalies, intrusions, and malware that compromise infrastructures. Particularly, intrusion detection emerged as the most frequently targeted threat, with models designed to identify abnormal traffic patterns, malicious payloads, and suspicious users' activities. Two of the final selected studies (Ofili *et al*., 2024) highlight how predictive AI models are deployed to recognize unauthorized access attempts and behavioral deviations within cloud platforms. Some of the final selected studies (Nallah, 2023; Stutz *et al*., 2024) underscore ransomware and data integrity attacks, especially within sensitive sectors such as healthcare system where predictive systems track irregularities in health record modifications. Moreover, the study showed that phishing, identity fraud and IoT-enhanced attacks are threats observed in cloud systems (Ayyadapu, 2023). This demonstrates that predictive AI approaches are increasingly generalized across heterogeneous cloud threat landscapes, indicating their adaptability to evolving cybersecurity risks. This pattern suggests that predictive AI research prioritizes proactive threat detection capabilities, reflecting the shift from reactive security mechanisms toward predictive and behaviour-based defence strategies.

Regarding Research Question 2, the findings indicate the adoption of a diverse spectrum of predictive AI models ranging from conventional machine learning algorithms to advanced deep learning architectures. This ranges from traditional machine learning techniques to more advanced deep learning techniques. Some of the deep learning models prominently used include CNNs, LSTMs, BiLSTMs, and Transformers, especially in hybrid forms that combine temporal, spatial, and contextual learning patterns (Abdul *et al*., 2023; Sourag & Sagayam, 2024). For instance, Sudhakar *et al*. (2025) integrated CNN, BiLSTM, and Transformer layers to create CloudSecureNet, which is a robust threat detection model capable of extracting deep hierarchical features from network traffic. It was shown from the studies that traditional learning models like Random Forests, SVMs, Naïve Bayes, and Decision Trees were used for threats identification (Abdul *et al*., 2023; Ayyadapu, 2023). These traditional learning models are often used as ensemble components alongside deep learning feature extractors, as demonstrated in architectures such as CloudSecureAI and other similar architectures. Moreover, some studies (Aldawsari & Kouchay, 2023; Sourag & Sagayam, 2024) applied autoencoders and clustering algorithms for detecting unseen anomalies where labelled data are limited.

In relation to Research Question 3, the results indicate that predictive AI models substantially improve cloud security performance. The study showed that deep learning and hybrid systems outperform standalone traditional machine learning in accuracy, precision-recall balance, and detection robustness (Sudhakar *et al*., 2025). The study of Sudhakar *et al*. (2025) reported an accuracy level of 98.74%, while

other models demonstrate strong generalization across multiple datasets. The majority of the final selected studies (e.g. Aiswarya, 2021; Naidu *et al*., 2024; Nalla, 2023; Nina & Ethan, 2019) highlight reduced false positive rates, faster detection speeds, and enhanced real-time monitoring performance. This is, especially common in healthcare systems and IoT-cloud environments. Nevertheless, all of these studies concluded that the effectiveness of the predictive AI models hinges on controlled experiments rather than broad-scale industrial deployments. This finding underscores the need for future research focusing on large-scale operational validation within heterogeneous cloud infrastructures. Concerning Research Question 4, the findings identify a wide range of datasets used for training and evaluating predictive AI models in cloud security. The study showed that public intrusion detection datasets, which include UNSW-NB15, CIC-IDS2017 and CSE-CIC-IDS2018, are the most commonly used due to their standardization and structured labelling, which support benchmarking (Sudhakar *et al*., 2025). For some studies (Nallah, 2023; Ramakrishna, 2022), these datasets are supported with proprietary logs, which include Prometheus telemetry, cloud-service access logs, and domain-specific datasets such as electronic health-record modification logs. Ayyadapu (2023) noted that large-scale training corpus highlights substantial dataset sizes, which sometimes reach 110GB. The study showed that IoT telemetry datasets support models designed to detect edge-origin attacks that propagate into cloud infrastructures. The heavy dependence on benchmark datasets suggests a need for more realistic and continuously updated datasets capable of reflecting dynamic cloud environments.

These evaluation practices indicate a growing emphasis not only on predictive accuracy but also on operational reliability, explainability, and deployment readiness of AI-driven security systems. Some of the studies (Abdul *et al*., 2023; Naidu *et al*., 2024) emphasized on the importance of balancing precision and recall to manage false alarms, while other studies (Ramakrishna, 2022; Sudhakar *et al*., 2025) report improvements in inference latency and mean time to threat detection. Sudhakar *et al*. (2025) incorporated interpretability tools such as Shapley Additive exPlanations (SHAP) values and attention-weight visualization to enhance transparency, particularly in deep learning systems. These evaluation techniques demonstrate an interest in not only achieving high-performance results but also ensuring that predictive AI models can function effectively in operational contexts.

On the research question six, the findings showed that despite the benefits of using predictive AI models for cloud security/ numerous challenges remain associated with their implementation. The most common challenge observed is the prevalence of false positives, which can overwhelm security analysis and undermine operational efficiency (Naidu *et al*., 2024; Nalla, 2023). Ramakrishna (2022) showed that other challenges include a shortage of high-quality, labelled, and representative datasets, which can hamper model development. The study highlights how limitations of benchmarking datasets make it difficult to reflect real-world cloud conditions. Other challenges found include adversarial vulnerabilities, scalability constraints, and the computation cost of deep learning models, especially in high-throughput cloud environments (Ali *et al*., 2024; Kummara, 2025). Moreover, it was shown that there can be privacy and regulatory issues when handling sensitive log data, which may be from the complexity of integrity AI systems in cloud-native architecture (Oduri, 2019). Collectively, these challenges highlight the necessity for balanced integration of predictive AI systems that simultaneously address performance, scalability, ethical, and regulatory considerations.

4.0 Conclusion

This study systematically reviewed existing literature to examine how predictive artificial intelligence (AI) models enhance cloud security within contemporary cloud computing environments. The findings demonstrate that predictive AI represents a significant shift from traditional reactive security mechanisms toward proactive, data-driven threat detection and prevention strategies. Across the reviewed studies, predictive AI approaches were consistently applied to address major cloud security vulnerabilities, particularly anomaly-based intrusions, malware propagation, unauthorized access, phishing attacks, and IoT-enabled threats, reflecting the increasing complexity and dynamic nature of modern cloud infrastructures.

The review further reveals that cloud security research increasingly relies on advanced deep learning architectures—including Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), BiLSTMs, and Transformer-based models—often integrated within hybrid and ensemble frameworks. These models demonstrate superior performance compared to conventional machine learning techniques, achieving improved detection accuracy, balanced precision–recall performance, reduced false-positive rates, and faster response times. The widespread use of benchmark intrusion datasets and standardized evaluation metrics also indicates a growing effort toward methodological consistency and comparative validation within the field.

Despite these advancements, the study identifies several persistent limitations that constrain the practical deployment of predictive AI in real-world cloud environments. Key challenges include dependence on limited and highly controlled datasets, susceptibility to adversarial attacks, scalability and computational constraints, and privacy concerns associated with sensitive cloud data. The predominance of experimental evaluations over large-scale industrial implementations further highlights a critical gap between research outcomes and operational cloud security practice.

Overall, the study establishes that predictive AI models substantially strengthen cloud security capabilities but require continued refinement to achieve reliable, scalable, and ethically responsible deployment. Future research should prioritize the development of representative real-world datasets, explainable and interpretable AI models, adaptive learning mechanisms, and resilient architectures capable of operating effectively within heterogeneous cloud ecosystems. Addressing these challenges will be essential for fully realizing the transformative potential of predictive AI in securing next-generation cloud infrastructures.

5.0 References

Abdul, S., Ismail, B. I., Khan, S. M., Sattar, S. A., & Muhammad, S. (2023). Assessing AI-based threat detection in cloud security. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, 14, 1, pp. 133-154.

Adeyemi, D. S. (2024). Effectiveness of machine learning models in intrusion detection systems: A systematic review. *Communication in Physical Sciences*, 11, 4, pp. 1060-1088.

Adeyemi, I. O., Akanbi, M. L., & Issa, A. O. (2025). Influence of game literacy on gamified library services: A systematic review of literature. *Alexandria, XX, X,* pp. , 1-18.

Aiswarya, R. S. (2021). Cloud infrastructure security using AI-powered threat prediction and mitigation. *Journal of Techno Social*, 13, 1, pp. 66-74.

Akinade, A. O., Adepoju, P. A., Ige, A. B., & Afolabi, A. I. (2025). Cloud security challenges and solutions: A review of current best practices. *International*

Journal of Multidisciplinary Research Growth Evaluation, 6, 1, pp. 26-35.

Alani, M. M. (2016). *Elements of cloud computing security: A survey of key practicalities*. Springer International Publishing.

Aldawsari, H., & Kouchay, S. A. (2023). Integrating AI and machine learning algorithms in cloud security frameworks for enhanced proactive threat detection and mitigation. *Journal of Emerging Threat Management*, 74, pp. 1042-1059.

Ali, A. R. A. R., Saravanan, K., Abirami, B. B., Pandi, V. S., Aroulanandam, V. V., & Parthiban, S. (2024). Enhancing cloud security with AI: developing robust, scalable solutions for threat mitigation and data protection in cloud platforms. In *2024 International Conference On Sustainable Communication Networks and Application (ICSCNA)* (pp. 614-620). IEEE.

Amir-Behghadami, M., & Sadeghi-Bazarghani, H. (2021). Why and how to apply exploratory sequential mixed methods in health-related psychometric research. *BMJ Supportive & Palliative Care*, 14, e3, pp. e3033-e3035.doi: 10.1136/bmjspcare-2021-003170

Attou, H., Mohy-eddine, M., Guezzaz, A., Benkirane, S., Azrour, M., Alabdultif, A., & Almusallam, N. (2023). Towards an intelligent intrusion detection system to detect malicious activities in cloud computing. *Applied Sciences*, 13, 17,. https://doi.org/10.3390/app13179588

Ayyadapu, A. K. R. (2023). Enhancing cloud security with AI-driven big data analytics. *International Neurourology Journal*, 27, 4, pp. 1591-1597.

Birje, M. N., Challagidad, P. S., Goudar, R. H., & Tapale, M. T. (2017). Cloud computing review: concepts, technology, challenges and security. *International Journal of Cloud Computing*, 6, 1, pp. 32-57.

Butt, U. A., Amin, R., Mehmood, M., Aldabbas, H., Alharbi, M. T., & Albaqami, N. (2023). Cloud security threats and solutions: A survey. *Wireless Personal Communications*, 128, 1, pp. 387-413.

Duncan, A., Creese, S., & Goldsmith, M. (2015). An overview of insider attacks in cloud computing. *Concurrency and Computation: Practice and Experience*, *27*, 12, pp. 2964-2981.

Kumari, S. (2022). AI-Driven cybersecurity in agile cloud transformation: Leveraging machine learning to automate threat detection, vulnerability management, and incident response. *Journal of Artificial Intelligence Research*, *2*(1), 286-305.

Kummara, R. (2025). Cloud security using AI: Transforming digital protection in the modern era. *Journal of International Crisis and Risk Communication Research*, 8, S9, pp. 27-36.

Maroc, S., & Zhang, J. (2019). Comparative analysis of cloud security classifications, taxonomies, and ontologies. In *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science* (pp. 666-672).

Murthy, J. S., Siddesh, G. M., & Srinivasa, K. G. (2024). *Cloud Security: Concepts, Applications and Practices*. CRC Press.

Naidu, P. R., Gowda, V. D., Gujar, S. S., Shaikh, S. F., Shandilya, S., & Reddy, N. S. (2024). AI-enhanced cloud security framework for IoT networks using a predictive analytics approach. In *2024 3rd International Conference for Advancement in Technology (ICONAT)* (pp. 1-8). IEEE.

Nalla, K. K. (2023). Predictive analytics with AI for cloud security risk management. *World Journal of Advanced Engineering Technology and Sciences*, 10, 2, pp. 297-308.

Nina, P., & Ethan, K. (2019). AI-driven threat detection: Enhancing cloud security with

cutting-edge technologies. *International Journal of Trend in Scientific Research and Development*, 4, 1, pp. 1362-1374.

Nwoye, C. C., & Nwagwughiagwu, S. (2024). AI-driven anomaly detection for proactive cybersecurity and data breach prevention. *International Journal of Engineering Technology Research & Management*, 8, 11, pp. 339-356.

Oduri, S. (2019). AI-driven security protocols for modern cloud engineers. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *10*(2), 2002-2008.

Ofili, B. T., Obasuyi, O. T., & Osaruwenese, E. (2024). Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. *International Journal of Engineering Technology Resource & Management*, 8, 11, pp. 631-645.

Parisa, S. K., & Banerjee, S. (2024). AI-enabled cloud security solutions: A comparative review of traditional vs. next-generation approaches.. International Journal of Statistical Computation and Simulation, 16, 1, pp. 1-15.

Polamarasetti, A. (2024). Role of artificial intelligence and machine learning to enhancing cloud security. In *2024 International Conference on Intelligent Computing and Emerging Communication Technologies (ICEC)* (pp. 1-6). IEEE.

Ramakrishna, S. (2022). AI-augmented cloud performance metrics with integrated caching and transaction analytics for superior project monitoring and quality assurance. *International Journal of Engineering & Extended Technologies Research*, 4, 6, pp. 5647-5655.

Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *Neuro Quantology*, 19, 12, pp. 764-773.

Salman, T., Bhamare, D., Erbad, A., Jain, R., & Samaka, M. (2017). Machine learning for anomaly detection and categorization in multi-cloud environments. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 97-103). IEEE.

Samarati, P., & De Capitani di Vimercati, S. (2016). Cloud security: Issues and concerns. *Encyclopedia of Cloud Computing*, pp. 205-219.

Schut, M., Adeyemi, I., Kumpf, B., Proud, E., Dror, I., Barrett, C. B., … Leeuwis, C. (2025). Innovation portfolio management for the public non-profit research and development sector: What can we learn from the private sector? *Innovation and Development*, 15, 3, pp. 689–707. https://doi.org/10.1080/2157930X.2024.2400779

Sharma, C., & Sharma, C. (2024). Cloud computing security: Threats and mitigation strategies. In *2024 International Conference on Signal Processing and Advance Research in Computing (SPARC)* (Vol. 1, pp. 1-6). IEEE.

Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, pp. 88-115.

Sokolov, S. A., Iliev, T. B., & Stoyanov, I. S. (2019). Analysis of cybersecurity threats in cloud applications using deep learning techniques. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 441-446). IEEE.

Sourag, V. T., & Sagayam, M. S. (2024). Investigating how AI and machine learning can be leveraged to enhance cloud security by predicting and preventing cyber threats. *Frightening Future of Business Researches in Public*

Policy and Social Science Domains, 9, 2, 119-134.

Stutz, D., de Assis, J. T., Laghari, A. A., Khan, A. A., Andreopoulos, N., Terziev, A., ... & Grata, E. G. (2024). Deshpande; Dhanashree Kulkarni; Edwiges G.H. Grata, "Enhancing Security in Cloud Computing Using Artificial Intelligence (AI)," in *Applying Artificial Intelligence in Cybersecurity Analytics and Cyber Threat Detection* , Wiley, 2024, pp.179-220, doi: 10.1002/9781394196470.ch11.

Sudhakar, G., Chandra Shekhar Rao, V., Sunitha, M., Pulipati, V., & Santhosh Kumar, R. (2025). Hybrid AI-based threat prediction and mitigation framework for securing cloud storage. *The European Physical Journal Plus*, 140, 10, pp. 1-26.

Sunyaev, A. (2020). Cloud computing. In *Internet computing* (pp. 195-236). Springer, Cham.

Tissir, N., El Kafhali, S., & Aboutabit, N. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments*, 7, 2, pp. 69-84.

Vashishth, T. K., Sharma, V., Sharma, K. K., Kumar, B., Chaudhary, S., & Panwar, R. (2024). Enhancing cloud security: The role of artificial intelligence and machine learning. In *Improving security, privacy, and trust in cloud computing* (pp. 85-112). IGI Global Scientific Publishing.

Zhang, N., Liu, D., & Zhang, Y. (2013). A research on cloud computing security. In *2013 International Conference on Information Technology and Applications* (pp. 370-373). IEEE.

Declaration

Consent for publication

Not Applicable

Availability of data and materials

The publisher has the right to make the data public

Conflict of Interest

The authors declared no conflict of interest

Ethical Considerations

Not applicable

Competing interest

The authors report no conflict or competing interest

Funding

The author declared no source of funding

Authors' Contributions

All components of the work were carried out by the author.