International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)
https://ijcjournal.org/index.php/InternationalJournalOfComputer/index

Leveraging AI Techniques to Enhance Data Security in Cloud Environments: Challenges and Future Prospects

Olushola Adegoke [a]*, Abiola Adedeji Adebanjo [b], Grace Durotolu [c]

[a,b] *Harrisburg University of Science and Technology, 326 Mkt St, Harrisburg PA 17101, United States*
[c] *Troy University, 600 University Ave, Troy, AL 36082*
[a]*Email: Shuks2004@yahoo.com*
[b]*Email: abiolar.adebanjo@gmail.com*
[c]*Email: jdurotolu@yahoo.com*

Abstract

This paper explores the application of Artificial Intelligence (AI) techniques to enhance data security in cloud computing environments. As organizations increasingly migrate to the cloud, the need for robust security measures has become paramount. Traditional security approaches often struggle to keep pace with the dynamic nature of cloud environments and sophisticated cyber threats. This research examines how AI can address these challenges and improve cloud security. The study analyzes the current state of AI applications in cloud security, evaluates key AI techniques applicable to various cloud security challenges, and identifies future directions for AI integration in cloud security. Machine learning, natural language processing, and other AI methods are discussed in the context of threat detection, anomaly identification, and adaptive security measures. While highlighting the potential of AI in cloud security, the paper also addresses significant challenges, including data quality issues, model interpretability, adversarial attacks on AI systems, privacy concerns, integration with legacy systems, and the cybersecurity skills gap. The research concludes by proposing future directions, such as quantum-resistant AI, federated learning for collaborative security, AI-driven autonomous security systems, and the development of explainable AI for security applications. This comprehensive analysis provides valuable insights for cloud service providers, enterprise customers, cybersecurity professionals, and policymakers navigating the rapidly evolving landscape of AI-driven cloud security.

Keywords: Artificial Intelligence; Cloud Computing; Cybersecurity.

Received: 9/1/2024
Accepted: 11/1/2024
Published: 11/11/2024

----

* Corresponding author.

1. Introduction

In an era when data is now considered the “new oil” [1], the security of this invaluable resource has become paramount. As organizations increasingly migrate their operations to the cloud, the landscape of data security is undergoing a profound transformation [2]. With 71% of enterprises now considered “heavy users” of public cloud services [3] and cyberattacks surging by 300% since the onset of the COVID-19 pandemic [4], the imperative to secure data in cloud environments has never been more critical.Cloud computing is one of the key technologies enabling digital transformation in business operations [5]. The global cloud market, valued at $626.4 billion in 2023, is projected to reach $1.266 trillion by 2028 [6], underscoring the rapid adoption of cloud technologies across industries. However, this shift also introduced novel and complex security challenges [2], including data breaches, compliance issues, and threats from malicious insiders [7]. The distributed nature of cloud infrastructure and the vast amounts of sensitive data now stored in the cloud have combined to create a breeding ground for security and privacy breaches [8].Traditional security measures, while still relevant, are often insufficient to address the unique challenges posed by cloud environments [2,9,10]. The sheer volume and velocity of data generated in the cloud [11], coupled with the dynamic nature of cloud resources, demand a more adaptive and intelligent approach to security [12,13]. This is where Artificial Intelligence (AI) emerges as a game-changing technology in the realm of cloud security [14].

AI, with its ability to process and analyze vast amounts of data in real-time [15] holds immense potential in enhancing cloud security. From anomaly detection [16] to predictive analytics [17], AI techniques offer a powerful toolkit for securing cloud environments. This research aims to explore a simple, but critical, question: How can artificial intelligence techniques be effectively leveraged to enhance data security in cloud computing environments?

The study’s objectives are to:

1. Analyze the current state of AI applications in cloud security.

2. Identify and evaluate key AI techniques applicable to various cloud security challenges.

3. Identify challenges and propose future directions for AI integration in cloud security.

The significance of this research lies in its timely exploration of AI's potential to revolutionize cloud security practices. As organizations continue to increase their reliance on cloud services, the insights provided by this study will be valuable to cloud service providers, enterprise customers, cybersecurity professionals, and policymakers alike.

2. Previous Studies and Related Work

The intersection of cloud computing and artificial intelligence represents a frontier in cybersecurity, blending the vast scalability of cloud environments with the adaptive intelligence of AI [18,19]. A review of relevant literature reveals a growing body of research exploring AI applications in cloud security. To fully appreciate the potential of this synergy and the problems inherent in it, it is crucial to first understand the current state of data security in cloud environments and the evolving role of AI in cybersecurity.

2.1 The Current State of Data Security in Cloud Environments

Current security measures in cloud environments encompass a range of technologies and practices, such as the shared responsibility model as well as encryption, access controls, identity management, and cloud governance Reference [20]. These measures address issues like data breaches, insider threat, malware injection, unauthorized access, insecure APIs, insufficient due diligence, shared vulnerability, and compliance with regulatory standards Reference [20].

The shared responsibility model—the cornerstone of cloud security [9,20]—entails the delineation of security obligations between cloud service providers and their customers [21]. Encryption serves as a primary method for protecting data in cloud environments [20], ensuring both data in transit and data at rest [22], and, more recently, data in usage [23] are secure. Access control and identity management systems gatekeep cloud resources, manage user identities, and control access to sensitive data [20,24,25,26]. Firewalls and intrusion detection systems protect cloud environments by monitoring for threats and unauthorized access [10,27]. Rounding out the standard security toolkit, IT auditing mechanisms [28,29,30] play important roles in compliance checks and adherence to security policies and regulations.

2.2 The Evolving Role of AI in Cybersecurity

However, as noted earlier, these traditional measures often struggle to keep pace with the dynamic nature of cloud environments and the sophistication of modern cyber threats [13,31,32]. Thus, the evolution of cloud security has been marked by a shift from perimeter-based defenses to more distributed and adaptive approaches [33]. This transition aligns well with the capabilities of AI, which has already made significant inroads in various aspects of cybersecurity [31,32].Some of the applications of AI in cloud security contexts range from network traffic analysis to malware threat detection to privacy preservation. Saha, Haque, and Sidebottom [34] demonstrated that deep sequence models, which have hitherto been successfully used to predict complex IP traffic, can also be effectively utilized for anomalous traffic prediction. Their work showed promising results in detecting potential security threats by analyzing patterns in network traffic data. Similarly, Sleem and Elhenawy [35] explored the use of federated learning, a privacy-preserving approach, for collaborative cyber threat intelligence sharing among cloud tenants while maintaining data privacy. This approach allows multiple parties to train machine learning models on their local data without sharing the raw information.

3. AI Techniques for Cloud Data Security

The application of Artificial Intelligence (AI) in cloud data security represents a paradigm shift in how organizations and industries approach the protection of sensitive information in distributed environments. This section introduces some AI techniques that are being leveraged to enhance data security in cloud computing.

Machine Learning (ML) techniques form the backbone of many AI-driven security solutions in cloud environments. Supervised learning algorithms, such as Support Vector Machine, SVM [36] and eXtreme Gradient Boosting, XGBoost [37], have been successfully applied to classification problems in cloud computing security contexts. Other supervised ML techniques, like Random Forest and k-Nearest Neighbors (k-NN) classifiers, have shown particular promise in enhancing network security, especially in IoT-based cloud computing systems, by analyzing traffic patterns, detecting anomalies, and identifying potential threats [38]. These models excel in scenarios where labeled data is available, making them particularly useful for known threat detection.Unsupervised machine learning techniques, on the other hand, are particularly effective for anomaly detection, a critical component of cloud security [39]. They excel in identifying unusual patterns that could indicate security threats without prior knowledge or the need for labeled data [40].Natural Language Processing (NLP) has emerged as a powerful tool for analyzing security logs and processing threat intelligence. NLP has been effectively used to analyze system logs and detect anomalies, which helps in preventing and mitigating information security events in real time. By employing NLP techniques such as doc2vec, these methods can extract semantic information from logs and apply classification algorithms for anomaly detection [41].NLP techniques are also valuable for processing security logs and categorizing threat intelligence in cloud security contexts. These techniques enable the automated extraction of insights from unstructured data, which is crucial for effective security management [42].

4. Challenges

While AI has demonstrated immense potential in enhancing cloud security, its implementation and ongoing development face several significant challenges. This section explores these challenges.

4.1 Data Quality and Availability

The success of AI models in accurately predicting and mitigating security threats heavily depends on the quality and quantity of the training data used [43]. High-quality and diverse [44,45], as well as accurately labeled datasets Reference [46] that represent the full spectrum of normal operations and potential threats are essential for developing robust AI models capable of handling various cloud security scenarios.

4.2 Model Interpretability and Explainability

As AI models grow in complexity, the need for their decisions to be interpretable and explainable to human operators is paramount. The work of Veprytska and Kharchenko [47] on developing a model for evaluating eXplainable AI as a service (XAIaaS) emphasizes the need for quality assessment for an AI system, particularly in high-stakes security scenarios. Also, ensuring that AI decisions can be understood by humans is crucial for user trust in AI and information security, with implications for ethics and informed consent [48]. Pieters [48] highlights the importance of transparency in AI decision-making processes. This transparency is critical not only for maintaining trust but also for complying with regulatory requirements in security contexts.

4.3 Adversarial AI and AI-powered Attacks

As AI systems become integral to security measures, they themselves become targets for adversarial attacks, which aim to exploit vulnerabilities in AI models [49,50]. Aiken and Scott-Hayward [49] demonstrated how a carefully crafted adversarial test tool could completely fool a state-of-the-art, machine-learning based network intrusion detection systems (ML-NIDS), highlighting the need for robust, adaptive AI models that can withstand such attacks, like the ones demonstrated by Pawlicki and his colleagues [50], Cheolhee Park and his colleagues Reference [51], and He and his colleagues [52].

4.4 Privacy Concerns

The use of AI for security purposes often involves handling large volumes of sensitive data, which raises significant privacy concerns. This issue is particularly pressing as AI systems require extensive data to function effectively, leading to potential risks of data breaches and misuse. Balancing the need for comprehensive security analysis while adhering to stringent data privacy regulations such as the GDPR presents ongoing challenges. The need to protect personal data must be balanced with the requirement to analyze and respond to security threats effectively.Bielova and Byelov [53] explores challenges and threats in personal data protection when working with artificial intelligence, recommending strict rules, encryption, and user awareness for data protection.

4.5 Integration with Legacy Systems

Many organizations struggle to integrate AI-driven security solutions with existing legacy infrastructure. Integrating AI-driven security solutions with legacy systems presents significant challenges due to differences in technology, architecture, and the complexity of existing systems. This integration is critical for enhancing security but requires overcoming substantial technical and operational hurdles. However, innovative solutions and strategies, like the ones presented by Singh and Adhikari [54], can address these barriers, leading to successful inventory management in traditional industries.

4.6 Skill Gap

The shortage of professionals with simultaneous expertise in both AI and cloud security presents a significant challenge to the widespread adoption and effective implementation of AI-driven security solutions. This shortage is a significant hurdle to the effective adoption and implementation of AI-driven security solutions. Many organizations struggle to find and retain talent with the necessary combination of skills [55].

5. Future Directions

This section outlines future directions for research and development in AI-driven cloud security.

5.1 Quantum-Resistant AI

As quantum computing technology advances, it is essential to develop AI models that can effectively function within post-quantum cryptographic frameworks to ensure continued security and performance [56]. Results of the work by Wan and his colleagues [57] shows AI accelerators, such as NVIDIA's Tensor Core, can significantly improve the performance of cryptographic computations, achieving speedups of 26x, 36x, and 35x for each phase compared to the state-of-the-art implementation.

5.2 Federated AI for Collaborative Security

Future research should enhance federated learning techniques to improve collaborative threat detection and response across different organizations and cloud providers while ensuring data privacy, as indicated earlier in this paper (2.2) by Sleem and Elhenawy [35] and likewise by the work of Tian and his colleagues [58].

5.3 AI-Driven Autonomous Security Systems

The advancement of fully autonomous AI security systems capable of detecting, analyzing, and responding to threats with minimal human intervention is a significant step forward in cybersecurity. These systems promise to enhance the efficiency and effectiveness of threat management. Havenga and his colleagues [59] tested an Autonomous Threat Detection and Response (ATDR) system that accurately classifies network traffic in real-time, effectively isolating malicious traffic flows and reducing wait time with minimal traffic delay.

5.4 Explainable AI for Security

Advancing explainable AI for security applications is essential to ensure that AI models can provide clear and actionable explanations for their decisions. This transparency is vital for building trust and ensuring the effective use of AI in high-stakes security contexts. Future research should focus on developing AI models that can make accurate security decisions and also provide clear, actionable explanations. This dual capability is crucial for maintaining trust and compliance with regulatory requirements in security applications. A relatively recent survey research article [60] provided a comprehensive overview of Explainable Artificial Intelligence (XAI) methods for cyber security, aiming to enhance transparency and interpretability while maintaining high accuracy in defense against cyber-attacks.

5.5 Bio-Inspired AI for Adaptive Security

AI security systems that can adapt and evolve in response to new threats, inspired by biological immune systems, represent a promising direction for future cybersecurity advancements. These systems could automatically adjust their defenses to counteract evolving cyber threats. A notable example representative of these cutting-edge technologies was featured in Nicolaou and his colleagues [61].

5.6 Edge AI for Distributed Cloud Security

The growing adoption of edge computing necessitates the development of efficient AI models capable of operating effectively at the edge and coordinating with central cloud systems. This ensures robust and scalable AI-driven solutions for various applications. The intelligent cooperative edge computing architecture enables a complementary integration of AI and edge computing, enabling better solutions for computation offloading and content caching in IoT networks [62].

5.7 Ethical AI in Security

Future research must address the ethical implications of AI in security contexts, particularly issues of bias, fairness, and accountability. These concerns are critical to ensure that AI systems do not perpetuate or exacerbate existing inequalities and are used responsibly. AI systems must be transparent and understandable to combat bias and ensure fairness, while balancing justice and efficacy in decision-making [63].

The field of AI-driven cloud security is rapidly evolving, and addressing these challenges while pursuing the future directions will require ongoing collaboration between researchers, industry practitioners, policymakers, and ethicists. As we navigate this complex landscape, the ultimate goal remains clear: to harness the power of AI to create more secure, trustworthy, and resilient cloud ecosystems.

6. Conclusion

The integration of Artificial Intelligence (AI) with cloud security represents a paradigm shift in how we approach the protection of data and resources in distributed computing environments. Throughout this paper, the multifaceted applications of AI in enhancing cloud security, from threat detection and privacy preservation to compliance monitoring and autonomous response systems were explored.

The analysis revealed that AI techniques, when properly implemented, can significantly improve the accuracy, speed, and adaptability of cloud security measures. Machine learning algorithms have demonstrated remarkable efficacy in detecting anomalies and identifying potential threats, often outperforming traditional rule-based systems. Deep learning models have shown promise in processing and analyzing vast amounts of complex data, enabling more sophisticated threat intelligence and predictive security capabilities.

However, examination also highlighted significant challenges that must be addressed as AI applications in cloud security are implemented. The issues of data quality, model interpretability, and the potential for adversarial attacks on AI systems themselves present ongoing concerns. Moreover, the ethical implications of AI in security contexts, particularly regarding privacy and fairness, require careful consideration and proactive management.

Looking to the future, several promising directions emerge. The development of quantum-resistant AI, the advancement of federated learning for collaborative security, and the integration of AI with edge computing all offer exciting possibilities for further enhancing cloud security. The potential for fully autonomous AI security systems, while still in its early stages, could revolutionize how we approach threat detection and response in cloud environments. It is crucial to recognize that AI is not a panacea for all cloud security challenges. The most effective approaches will likely combine AI-driven solutions with traditional security measures and human expertise. AI in cloud security should be viewed not as a replacement for human insight, but as a powerful tool that augments and enhances our ability to protect digital assets in increasingly complex environments.

Ultimately, the role of AI in cloud security is set to grow increasingly important in the coming years. As cloud adoption continues to accelerate across industries, the need for more sophisticated, adaptive, and intelligent security measures becomes paramount. By addressing current challenges and pursuing innovative research directions, organizations can harness the full potential of AI to create more secure, resilient, and trustworthy cloud ecosystems.

7. Constraints and Limitations of the Study

Here's a summary of the key constraints and limitations identified in this study:

1. Broad scope potentially limiting depth in specific areas
2. Reliance on literature review and theoretical analysis rather than original empirical research
3. Rapid technological evolution potentially dating some findings
4. Limited discussion of practical implementation challenges in real-world cloud environments
5. Lack of detailed cost-benefit analysis of implementing AI-driven security solutions in cloud environments
6. Limited exploration of regulatory and compliance issues

These constraints and limitations don't negate the value of the study, but addressing them in future research would provide a more comprehensive understanding of AI applications in cloud security.

7.1 Scope and Depth:

While providing a comprehensive overview, the paper may not dive deeply into the technical intricacies of each AI method or security challenge.

7.2 Empirical Evidence:

Lack of original quantitative data or case studies may limit the practical validation of the proposed AI applications in cloud security.

7.3 Rapid Technological Evolution:

The field of AI and cloud security is rapidly evolving. The study's findings and recommendations may become outdated quickly, thus unable to capture the most recent developments in AI and cloud security.

7.4 Implementation Challenges:

The paper could benefit from more in-depth discussion of integration issues with existing cloud infrastructure and legacy systems.

7.5 Cost-Benefit Analysis:

Lack of economic considerations may limit the study's practical applicability for organizations considering AI adoption in their cloud security strategies.

7.6 Regulatory and Compliance Issues:

While the study touches on compliance, it could benefit from a more detailed examination of how AI-driven security solutions align with various international data protection regulations and industry standards.

Despite these limitations, the study provides valuable insights into the current state and future prospects of AI in cloud security. Addressing these constraints in future research would further enhance our understanding of this critical field.

References

[1] "The world's most valuable resource is no longer oil, but data," The Economist, May 6, 2017. [Online]. Available: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data

[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

[3] Flexera, "State of the Cloud Report," 2024. [Online]. Available: https://info.flexera.com/CM-REPORT-State-of-the-Cloud

[4] FBI (Federal Bureau of Investigation), "Internet Crime Report 2022," 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[5] H. Mydyti, J. Ajdari, and X. Zenuni, "Cloud-based Services Approach as Accelerator in Empowering Digital Transformation," in 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), 2020, pp. 1390-1396.

[6] MarketsandMarkets, "Cloud Computing Market - Global Forecast to 2028," 2023. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html

[7] K. Kifayat, M. Merabti, and Q. Shi, "Future security challenges in cloud computing," Int. J. Multim. Intell. Secur., vol. 1, pp. 428-442, 2010.

[8] H. Takabi, J. B. Joshi, and G. Ahn, "Security and privacy challenges in cloud computing environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24–31, 2010.

[9] D. Bird, "Derivation of a Conceptual Framework to Assess and Mitigate Identified Customer Cybersecurity Risks by Utilizing the Public Cloud," in International Congress on Information and Communication Technology, 2019, pp. 249-265.

[10] M. Humphrey, R. Emerson, and N. Beekwilder, "Unified, Multi-level Intrusion Detection in Private Cloud Infrastructures," in 2016 IEEE International Conference on Smart Cloud (SmartCloud), 2016, pp.

11-15.

[11] K. Benzidane et al., "Toward a cloud-based security intelligence with big data processing," in NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, 2016, pp. 1089-1092.

[12] D. Gangwani, H. A. Sanghvi, V. Parmar, R. H. Patel, and A. S. Pandya, "A comprehensive review on cloud security using machine learning techniques," in Intelligent systems reference library, 2023, pp. 1–24.

[13] K. A. Torkura, M. I. Sukmana, F. Cheng, and C. Meinel, "SlingShot - Automated Threat Detection and Incident Response in Multi Cloud Storage Systems," in 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), 2019, pp. 1-5.

[14] N. Abbas, T. Ahmed, S. H. Shah, M. Omar, and H. W. Park, "Investigating the applications of artificial intelligence in cyber security," Scientometrics, vol. 121, pp. 1189-1211, 2019.

[15] C. Zhou, Q. Liu, and R. Zeng, "Novel defense schemes for artificial intelligence deployed in edge computing environment," Wireless Communications and Mobile Computing, vol. 2020, pp. 1–20, 2020.

[16] A. Libri, A. Bartolini, and L. Benini, "pAElla: Edge AI-Based Real-Time Malware Detection in Data Centers," IEEE Internet of Things Journal, vol. 7, pp. 9589-9599, 2020.

[17] M. P. Yadav, N. Pal, and D. K. Yadav, "Workload Prediction over Cloud Server using Time Series Data," in 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2021, pp. 267-272.

[18] X. Cao, "The application of artificial intelligence in internet security," Applied and Computational Engineering, 2023.

[19] A. Dhondse and S. Singh, "Redefining Cybersecurity with AI and Machine Learning," International Research Journal of Modernization in Engineering Technology and Science, 2023.

[20] J. Njoku, "A Proactive Approach to Addressing Security Challenges in Cloud Migration," Advances in Multidisciplinary and scientific Research Journal Publication, 2023.

[21] CloudPassage, "Shared responsibility model explained," Aug. 26, 2020. [Online]. Available: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained

[22] M. Dhingra, "Cloud Data Encryption Ensuring Security," International journal of engineering research and technology, vol. 4, 2015.

[23] K. Nandakumar et al., "Securing data in transit using data-in-transit defender architecture for cloud communication," Soft Computing, vol. 25, pp. 12343-12356, 2021.

[24] I. Indu and P. M. Rubesh Anand, "Identity and access management for cloud web services," in 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), 2015, pp. 406-410.

[25] F. M. Johnson, "Robust identity and access management for cloud systems," 2020.

[26] Y. Yang, X. Chen, G. Wang, and L. Cao, "An Identity and Access Management Architecture in Cloud," in 2014 Seventh International Symposium on Computational Intelligence and Design, vol. 2, 2014, pp. 200-203.

[27] X. Ma, X. Fu, B. Luo, X. Du, and M. Guizani, "A Design of Firewall Based on Feedback of Intrusion Detection System in Cloud Environment," in 2019 IEEE Global Communications Conference (GLOBECOM), 2019, pp. 1-6.

[28] Z. Chen and J. Yoon, "IT Auditing to Assure a Secure Cloud Computing," in 2010 6th World Congress on Services, 2010, pp. 253-259.

[29] I. Gul, A. ur Rehman, and M. H. Islam, "Cloud computing security auditing," in The 2nd International Conference on Next Generation Information Technology, 2011, pp. 143-148.

[30] Y. Wang, B. S. Rawal, and Q. Duan, "Securing Big Data in the Cloud with Integrated Auditing," in 2017 IEEE International Conference on Smart Cloud (SmartCloud), 2017, pp. 126-131.

[31] M. S. Hossen, T. Ahmad, and M. A. Rachman Putra, "Traffic Classification with Machine Learning for Enhancing Cloud Security," in 2023 Intelligent Methods, Systems, and Applications (IMSA), 2023, pp. 86-91.

[32] S. Rangaraju, "SECURE BY INTELLIGENCE: ENHANCING PRODUCTS WITH AI-DRIVEN SECURITY MEASURES," EPH - International Journal of Science And Engineering, 2023.

[33] M. Torquato and M. P. Vieira, "Towards Models for Availability and Security Evaluation of Cloud Computing with Moving Target Defense," ArXiv, abs/1909.01392, 2019.

[34] S. Saha, A. Haque, and G. Sidebottom, "Deep Sequence Modeling for Anomalous ISP Traffic Prediction," in ICC 2022 - IEEE International Conference on Communications, 2022, pp. 5439-5444.

[35] A. Sleem and I. Elhenawy, "Enhancing Cyber Threat Intelligence Sharing through a Privacy-Preserving Federated Learning Approach," Journal of Cybersecurity and Information Management, 2022.

[36] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine Learning for Cloud Security: A Systematic Review," IEEE Access, vol. 9, pp. 20717-20735, 2021.

[37] Z. Abbas and S. Myeong, "Enhancing Industrial Cyber Security, Focusing on Formulating a Practical Strategy for Making Predictions through Machine Learning Tools in Cloud Computing Environment,"

Electronics, 2023.

[38] H. Naeem, "Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning," International Journal for Electronic Crime Investigation, 2023.

[39] S. Shriram and E. Sivasankar, "Anomaly Detection on Shuttle data using Unsupervised Learning Techniques," in 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2019, pp. 221-225.

[40] G. Pu, L. Wang, J. Shen, and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," Tsinghua Science and Technology, 2021.

[41] M. Wang, L. Xu, and L. Guo, "Anomaly detection of software system logs based on natural language processing," Other Conferences, 2018.

[42] N. Afzaliseresht, Y. Miao, S. Michalska, Q. Liu, and H. Wang, "From logs to Stories: Human-Centred Data Mining for Cyber Threat Intelligence," IEEE Access, vol. 8, pp. 19089-19099, 2020.

[43] T. Y. Mohammed, "Impact of Number of Features Selected and Size of Training Data on the Accuracy of Machine Learning Based Cloud Security Algorithms -- An Empirical Analysis," SLU Journal of Science and Technology, 2022.

[44] A. Biró, S. M. Szilágyi, and L. Szilágyi, "Optimal Training Dataset Preparation for AI-Supported Multilanguage Real-Time OCRs Using Visual Methods," Applied Sciences, 2023.

[45] Y. Yao et al., "Towards Automatic Construction of Diverse, High-Quality Image Datasets," IEEE Transactions on Knowledge and Data Engineering, vol. 32, pp. 1199-1211, 2017.

[46] X. Wu, W. Zheng, X. Xia, and D. Lo, "Data Quality Matters: A Case Study on Data Label Correctness for Security Bug Report Prediction," IEEE Transactions on Software Engineering, vol. 48, pp. 2541-2556, 2022.

[47] O. Veprytska and V. Kharchenko, "Analysis of Requirements and Quality Modeloriented Assessment of the Explainable Ai As A Service," Èlektronnoe modelirovanie, 2022.

[48] W. Pieters, "Explanation and trust: what to tell the user in security and AI?," Ethics and Information Technology, vol. 13, pp. 53-64, 2011.

[49] J. Aiken and S. Scott-Hayward, "Investigating Adversarial Attacks against Network Intrusion Detection Systems in SDNs," in 2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2019, pp. 1-7.

[50] M. Pawlicki, M. Choraś, and R. Kozik, "Defending network intrusion detection systems against

adversarial evasion attacks," Future Gener. Comput. Syst., vol. 110, pp. 148-154, 2020.

[51] C. Park et al., "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks," IEEE Internet of Things Journal, vol. 10, pp. 2330-2345, 2023.

[52] K. He, D. D. Kim, and M. R. Asghar, "Adversarial Machine Learning for Network Intrusion Detection Systems: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 25, pp. 538-566, 2023.

[53] M. Bielova and D. Byelov, "Challenges and threats of personal data protection in working with artificial intelligence," Uzhhorod National University Herald. Series: Law, 2023.

[54] N. Singh and D. Adhikari, "Challenges and Solutions in Integrating AI with Legacy Inventory Systems," International Journal for Research in Applied Science and Engineering Technology, 2023.

[55] C. Nobles, "The Cyber Talent Gap and Cybersecurity Professionalizing," Cyber Warfare and Terrorism, 2020.

[56] I. Pedone, A. S. Atzeni, D. Canavese, and A. Lioy, "Toward a Complete Software Stack to Integrate Quantum Key Distribution in a Cloud Environment," IEEE Access, vol. 9, pp. 115270-115291, 2021.

[57] L. Wan et al., "A Novel High-performance Implementation of CRYSTALS-Kyber with AI Accelerator," IACR Cryptol. ePrint Arch., 2022, 881.

[58] P. Tian, Z. Chen, W. Yu, and W. Liao, "Towards asynchronous federated learning based threat detection: A DC-Adam approach," Comput. Secur., vol. 108, p. 102344, 2021.

[59] Havenga et al., "Autonomous Threat Detection and Response System," in Proceedings of the International Conference on Cybersecurity, 2022, pp. 123-130.

[60] Z. Zhang et al., "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," IEEE Access, vol. 10, pp. 93104-93139, 2022.

[61] A. Nicolaou, S. Shiaeles, and N. Savage, "Mitigating insider threats using Bio-Inspired models," Applied Sciences, vol. 10, no. 15, p. 5046, 2020.

[62] C. Gong, F. Lin, X. Gong, and Y. Lu, "Intelligent Cooperative Edge Computing in Internet of Things," IEEE Internet of Things Journal, vol. 7, pp. 9372-9382, 2020.

[63] N. Gupta, "Artificial Intelligence Ethics and Fairness: A study to address bias and fairness issues in AI systems, and the ethical implications of AI applications," Revista Review Index Journal of Multidisciplinary, 2023.