A Comprehensive Analysis on Cloud Security and Risk Management Using Artificial Intelligence

Name: MD Abdul Aziz

ID: 22-47013-1

Section: B

Semester: Fall 24-25

Motivation:

Cloud security as the silent bodyguard for your digital ecosystem. People Keep their private information in cloud so that it can be accessible from anywhere and most importantly to keep the information safe from getting leaked to any unauthorized person. But nowadays it is seen that many valuable information is leaking from cloud servers, which is a big reason to worry. It is an attack on the privacy of people. So, it is very important to ensure cloud security and manage the possible risks. Artificial intelligence can be a way of securing cloud and managing the risks. Artificial intelligence technology allows computers and machines to simulate human intelligence and problem-solving tasks. Artificial intelligence offers various models. These models can help us to predict security risks and can warn the user about the threat which can secure the data of the user and in future the same sort of threats can be minimized as well. The main purpose of this study is to secure the cloud environment so that everyone in the world can live without fear of violation and to make the cloud a secure place where users can store their valuable data with trust.

Literature Review:

Introduction:

Cloud data security is the practice of protecting data and other digital information assets from security threats, human error, and insider threats. The primary goals of cloud security include protecting data privacy and access control. It can spot unusual behavior, predict possible security threats, and respond to attacks much faster than humans can.

Related Works:

According to Nassif Et al.(2021) [1] , Traditional detection and prevention strategies are inadequate for dealing with both conventional and zero-day assaults, especially considering the massive data flows involved. To address these issues, the authors undertook a systematic literature review of machine learning approaches used in cloud security.

According to Kavitha Et al.(2021) [2] , According to Dr. S Kavitha et al., the study covers various important issues with security and privacy in Cloud computing and the Internet of Things. To propose a solution, the authors examine security risks and problems and provide solutions using the Logistic Regression algorithm.

According to Mohd Naved. et al.(2022)[3], the authors recognize that the main safety risk in Cloud systems is the inability of storage owners to control the location of their data, which creates worries about data privacy and protection. To solve the noted security issues, they go through a number of artificial intelligence models.

According to Thamer Abdel-Wahid Et al.(2024)[4], the authors focused on the difficulties of data privacy and the integration of artificial intelligence with existing security systems. To provide a solution, the author investigates the use of machine learning approaches to improve threat detection in cloud environment.

According to Olabanji Et al.(2024)[5], the paper observed that both AI-driven and traditional methods significantly enhance the accuracy of threat detection with traditional method showing a marginal superiority. The study proposed that organizations should adopt a hybrid approach in cloud security integrating both AI driven and traditional methods.

According to Reddy Et al.(2022)[6], deployable security measures are required since cloud infrastructures and service providers are the targets of cyberattacks . The paper proposes that AI-integrated cloud security can provide data-driven security through intelligent automation, transforming cybersecurity.

According to the journal by Reddy Et al.(2022)[7], artificial intelligence and cloud engineering, has opened new horizons in cybersecurity, offering opportunities to create defenses against cyber-attacks. The performance analysis of various classification models, including DT, SVM, and CNN-LSTM, shows a superior efficacy of CNN-LSTM model.

According to Jimmy Et al.(2023)[8], to address these risks, Cloud Security Posture Management has emerged as a strategic approach, helping organizations proactively manage and enhance their cloud security posture. The paper proposes that the integration of AI and Big Data into CSPM tools ensures a robust defense against security breaches, data loss, and unauthorized access.

According to Akinade Et al.(2025)[9], this review has explored the prevailing challenges and the best practices organizations are adopting to fortify their cloud environments. The paper suggests that securing the skies of cloud computing demands a concerted effort and a commitment to continuous improvement.

According to Akinbolaji Et al.(2024)[10], the integration of advanced artificial intelligence techniques for real-time threat detection offers a transformative approach to enhancing cybersecurity measures. The paper shows some limitations and computational resource requirements.

According to Butt Et al.(2020)[11], in this study, security threats and attacks as the most challenging issues in Clouds were analyzed. Different types of ML algorithms e.g., ANNs, K-NN, Naïve Bayes, SVM, K-Means, and SVD were investigated as solutions to address the security issues.

According to Palle Et al.(2014)[12], the exponential growth of data poses significant challenges for storage, leading many entities to migrate their data to cloud storage services. A lightweight optimal technique is proposed for constraints optimization.

According to KUNUNGO Et al.(2018)[13], The paper suggests that from managed machine learning platforms to specialized data processing engines, cloud providers offer a diverse array of solutions to streamline the development lifecycle.

According to Rangaraju Et al.(2023)[14], their research paper explores the integration of artificial intelligence strategies into the DevSecOps framework to enhance cloud security .The paper proposes that the integration of AI-driven techniques into DevSecOps represents a transformative soar towards providing the security.

According to Kunduru Et al.(2023)[15], this paper explores the advantages that Artificial Intelligence brings to cloud-based fintech application security. The paper proposes that despite challenges and risks, the benefits of AI in fintech application security are evident through real-world case studies and examples.

According to Belgaum Et al.(2021)[16], the paper discusses the role of artificial intelligence along with issues and opportunities confronting all communities. The paper suggests that this study will support researchers who choose to perform more work on some of the application combinations in the future.

According to Mazhar Et al.(2024)[17], the paper aims to provide a comprehensive understanding of the security challenges within Vehicular Cloud Computing. The paper suggests that the adaptive nature of AI techniques, including machine learning, deep learning, and anomaly detection, has been harnessed to create a comprehensive security framework.

According to Yathiraju(2022) [18], the study explored IT professionals' perceptions regarding the integration of AI and Supervised-machine (S-machine) learning into cloud service platforms in the enhancement of the cloud ERP system. This study provides a strong foundation for future research into organizations.

According to Aldhyani Et al. (2022)[19], The goal of their research is to enable the detection and effective mitigation of EDoS attacks . The paper proposes that the proposed systems are based on Machine Learning models for detecting EDoS attacks in cloud computing.

According to Elzamly Et al. (2017)[20], The aim of their study was to predict critical cloud computing security issues by using Artificial Neural Network (ANNs) algorithms. They presented the Levenberg–Marquardt based Back Propagation and LMBP algorithms to predict the performance for cloud security level.

Objective:

Main Objective:

To analyze the security challenges and risk management techniques in cloud computing environment with the aim of identifying effective solutions to handle risks and improve the security of cloud environments.

Sub Objectives:

1. To identify the security risks linked with cloud computing

2. To explore emerging technologies and tools for improving cloud security.
3. To evaluate existing methodologies for cloud security.
4. To examine the role of encryption and data protection techniques in cloud security.

Research Questions:

Main Question:

How can security challenges and risks in cloud computing be effectively managed to enhance the overall security of cloud environments?

Sub-Questions:

1. What are the major security risks associated with cloud computing?
2. What technologies and tools are available for improving cloud security?
3. How effective are current methodologies for ensuring cloud security?
4. What is the role of encryption techniques in cloud security?

Proposed Methodology:

Experimental methodology and model methodology can be used for analyzing cloud security issues and risk management techniques.

The experimental methodology can be used to examine the security concerns related to cloud computing to analyze real-world security incidents such as data breaches and unauthorized access. Case studies and cybersecurity reports from industry sources will be used to discover patterns and trends in cloud security concerns. Model methodology can be used to create a risk classification framework that classifies security risks based on their severity, likelihood, and potential impact on cloud settings.

To analyze emerging technologies and methods for increasing cloud security, an experimental methodology can be used to examine the performance of AI-driven threat detection. The experimental methodology will be used to observe the technologies and tools available for cloud computing in the real world. The model methodology can be used to create a structure that connects developing security technologies to cloud risks. The combination of experimental methodology and model methodology can be effective in observing the technologies available for improving cloud security.

To examine the effectiveness of current methodologies for ensuring cloud security both experimental and method methodology can be used. The effectiveness of existing cloud security methodologies can be assessed using an experimental methodology, where security frameworks will be evaluated based on real-world implementations. Additionally, model methodology can be used to develop a decision-making framework that will assist in selecting the most effective security approach based on their cloud architecture.

Encryption and data protection techniques play a crucial role in cloud security and their impact can be analyzed by using experimental methodology by analyzing case studies of encryption failures and successes. Experimental methodology can observe the case studies of the operation of encryption and then it can analyze the impact of encryption and data protection. Model methodology can also be used to identify the role of encryption techniques in cloud security. It can be used to create an encryption security model that matches the performance of several encryption algorithms in different attack situations.

References:

[1] Nassif, A.B., Talib, M.A., Nasir, Q., Albadani, H. and Dakalbab, F.M., 2021. Machine learning for cloud security: a systematic review. IEEE Access, 9, pp.20717-20735.

[2] Kavitha, S., Bora, A., Naved, M., Raj, K.B. and Singh, B.R.N., 2021. An internet of things for data security in cloud using artificial intelligence. International Journal of Grid and Distributed Computing, 14(1), pp.1257-1275.

[3] Naved, M., Fakih, A.H., Venkatesh, A.N., Vijayakumar, P. and Kshirsagar, P.R., 2022, May. Supervise the data security and performance in cloud using artificial intelligence. In AIP Conference Proceedings (Vol. 2393, No. 1). AIP Publishing.

[4] Abdel-Wahid, T., 2024. AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. International Journal of Information Technology and Electrical Engineering (IJITEE)-UGC Care List Group-I, 13(3), pp.11-19.

[5] Olabanji, S.O., Marquis, Y., Adigwe, C.S., Ajayi, S.A., Oladoyinbo, T.O. and Olaniyi, O.O., 2024. AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. Asian Journal of Research in Computer Science, 17(3), pp.57-74.

[6] Reddy, A.R.P., 2022. The Future of Cloud Security: Ai-Powered Threat Intelligence and Response. International Neurourology Journal, 26(4), pp.45-52.

[7] Reddy, M., Konkimalla, S., Rajaram, S.K., Bauskar, S.R., Sarisa, M. and Sunkara, J.R., 2022. Using AI And Machine Learning To Secure Cloud Networks: A Modern Approach To Cybersecurity. Available at SSRN 5045776.

[8] Jimmy, F.N.U., 2023. Cloud security posture management: tools and techniques. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online), 2(3).

[9] Akinade, A.O., Adepoju, P.A., Ige, A.B. and Afolabi, A.I., 2025. Cloud security challenges and solutions: A review of current best practices. Int J Multidiscip Res Growth Eval, 6(1), pp.26-35.

[10] Akinbolaji, T.J., 2024. Advanced integration of artificial intelligence and machine learning for real-time threat detection in cloud computing environments. Iconic Research and Engineering Journals, 6(10), pp.980-991.

[11] Butt, U.A., Mehmood, M., Shah, S.B.H., Amin, R., Shaukat, M.W., Raza, S.M., Suh, D.Y. and Piran, M.J., 2020. A review of machine learning algorithms for cloud computing security. Electronics, 9(9), p.1379.

[12] Palle, R.R., 2014. Lightweight Optimal Technique for Auditable Secure Cloud Using Hybrid Artificial Intelligence.

[13] KUNUNGO, S., RAMABHOTLA, S. and BHOYAR, M., 2018. The Integration of Data Engineering and Cloud Computing in the Age of Machine Learning and Artificial Intelligence.

[14] Rangaraju, S., Ness, S. and Dharmalingam, R., 2023. Incorporating AI-Driven Strategies in DevSecOps for Robust Cloud Security. International Journal of Innovative Science and Research Technology, 8(23592365), pp.10-5281.

[15] Kunduru, A.R., 2023. Artificial intelligence advantages in cloud Fintech application security. Central asian journal of mathematical theory and computer sciences, 4(8), pp.48-53.

[16] Belgaum, M.R., Alansari, Z., Musa, S., Alam, M.M. and Mazliham, M.S., 2021. Role of artificial intelligence in cloud computing, IoT and SDN: Reliability and scalability issues. International Journal of Electrical and Computer Engineering, 11(5), p.4458.

[17] Mazhar, N., 2024. Artificial Intelligence Techniques in Vehicular Cloud Computing Security. Integrated Journal of Science and Technology, 1(1), pp.9-9.

[18] Yathiraju, N., 2022. Investigating the use of an artificial intelligence model in an ERP cloud-based system. International Journal of Electrical, Electronics and Computers, 7(2), pp.1-26.

[19] Aldhyani, T.H. and Alkahtani, H., 2022. Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments. Sensors, 22(13), p.4685.

[20] Elzamly, A., Hussin, B., Abu-Naser, S.S., Shibutani, T. and Doheir, M., 2017. Predicting critical cloud computing security issues using Artificial Neural Network (ANNs) algorithms in banking organizations.