International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

The Role of AI in Enhancing Cloud Security: A Comprehensive Analysis of Its Impact on the Indian IT Industry

[1.] Syed Minhaj UI Hassan, [2.]Dr. Meena Chaudhary

Submitted: 03/05/2024 **Revised**: 16/06/2024 **Accepted**: 23/06/2024

Abstract: A rapidly expanding area of study, AI in cloud computing aims to provide smart solutions for various sectors. Businesses may use AI cloud computing's Machine Learning and Statistical capabilities to build dynamic apps with the power to execute complex computations. Artificial intelligence (AI) in the cloud is all about creating smart apps, assisting businesses with Big Data, using algorithms to make apps more powerful, and predicting and forecasting growth, which are huge boons to a company's bottom line and longevity. The article delves into the history of AI in cloud computing, how it has changed over time, the advantages it offers to big and small businesses, current market trends, examples of its application, and projections for the future.

Keywords: *Cloud Computing, Artificial Intelligence, Machine Learning, Internet of Things, Tesla, Algorithms, Linear Regression, Logistic Regression, Automated ML, Data Management, Synthetic Data, Analytics Platform*

1. Introduction

Organizations' top priority in this age of ubiquitous cloud computing and incessantly increasing digital data is protecting the authenticity and authenticity of their systems and data. Businesses' operations and data management have been radically altered by the appeal of cloud computing, which offers scalability, accessibility, and cost-efficiency. There are risks associated with this ease of use, however. Innovative technologies that can adapt and strengthen the cloud's defences are always needed to tackle the ever-changing cyber threat scenario. Although effective to a degree, traditional security procedures are needed when confronted with more complex threats. The answer is located at the crossroads of intellect and technology. AI and ML now lead cloud security due to their ability to sift through massive information, spot trends, and make real-time judgments. Starting with the ever-changing nature of cyber threats and moving on to the shortcomings of traditional security solutions, we seek to discover how AI and ML might revolutionize cloud security. We endeavour to provide cyber security experts and company executives with the understanding that they must protect their digital assets in this data-driven age by analyzing practical applications and discussing future issues. Come with us in our new episode and see how intelligence and technologies will save the entries to the cloud from the sharks of cloud security.

[1]*Research Scholar, Computer Science, Institute of Engineering and Technology, Mangalayatan University, Aligarh, UP, India*
20200937_syed@mangalayatan.edu.in
[2]*Asst. Professor, Institute of Engineering and Technology, Mangalayatan University, Aligarh, UP, India*
meena.chaudhary@mangalayatan.edu.in

Thus, data and system security has become one of the most significant priorities for enterprises nowadays due to the growth of digital data and the widespread usage of cloud technologies. Indeed, the possibilities of scaling, accessibility and cost-sharing have dramatically reshaped the business management of data and processes thanks to cloud computing. This ease, however, has its vices which must not be understated Samar (2006). Just like in any dynamic security situation, it is always useful to be able to come up with new creative solutions to adapt and strengthen the position of the cloud. Although they did to some extent, earlier security measures are different from today's morphology. When it comes to the meeting point of head and hand, the solution is always there. AI and ML have gained considerable traction in cloud security because of their capacity to sort through large volumes of information, identify trends, and make fast decisions. Following the analysis of the history of cyber threats and the inapplicability of traditional security solutions, this investigation proceeds with the exploration of the avant-garde opportunities of AI and MS for protecting cloud environments. Thus, this research will focus on the application of the existing systems and potential future problems as to sharp and effective preparation of cybersecurity specialists and corporate managers in the approaches to protect the digital resources. Follow us as we venture deeper into the cloudy waters of security and come out with a bright light, a future of AI and technology protecting the gates of the cloud.

2. Literature Review

Subramanian, E. K. , and Latha Tamilselvan [1] have built an understanding that paves way for the future generation of cloud security which is focused on

automated and responsive nature by proposing a new technique that employs the use of machine learning (ML) termed as the Convolutional neural network (CNN).

Fernandes [2], provide a good solution for categorizing such characteristics and also carries out a literature review of attacks, threats and vulnerabilities of cloud security.

To secure the private details and web-based programmes, Pavan [3] throws light on the security pattern of cloud computing in Muralidhara with new threats and their solutions.

Achar and Sandesh [4] delve into several facets of cloud computing models powered by artificial intelligence, including their forms, functions, current developments, and problems.

In his work, Nassif [5] delves into how machine learning methods might be used to detect and prevent security breaches in the cloud.

In his work, Khorshed [6] offers two main contributions: a thorough overview of cloud computing that focuses on obstacles to adoption and problems with threat mitigation and new ideas on using machine learning to tackle typical attack vectors.

To protect cloud-based virtual machines (VMs) against DoS assaults, Kumar, Raneel, Sunil Pranit Lal, and Alok Sharma [7] provide a method.

Using machine learning methods for time series forecasting and queuing theory, Moreno-Vozmediano introduces and evaluates [8] a new predictive auto-scaling mechanism.

Research by Dave et al. [9] illuminates cloud security concerns in various cloud-related fields, including dangers to cloud models and networks.

Nenvani, Geetanjali, and Huma Gupta [10] particularly emphasize the IaaS layer in their investigation of cloud computing security. The article addresses issues related to virtualization, such as attacks on VM image sharing, VM isolation violation, insecure VM migration, and VM escape. It also proposes remedies and thoroughly explores vulnerabilities inside IaaS.

The research by Hesamifard et al. [11] shows that training neural networks using encrypted data is both possible and practicable, which allows for encrypted predictions and the safe return of these predictions in encrypted form.

In their study, He, Zhang, and Lee [12] provide a method for detecting denial-of-service attacks in the cloud by using machine learning methods at the source.

Using supervised, unsupervised, semi-supervised, and reinforcement learning methods, among others, Butt and colleagues [13] provide a thorough analysis of cloud computing security risks, problems, and solutions.

Contrary to the prevalent practice in modern research, the researchers in Salman and [14] look at the identification and classification of outliers.

Artificial intelligence and machine learning are important when protecting data in the cloud and strengthening intrusion detection systems. Cloud cyber threat detection and mitigation using machine learning techniques such as Support Vector Machine, XGBoost, Artificial Neural Networks, Random Forest, and ensemble learning have been highlighted in several publications [15, 16, 17]. The general safety of cloud infrastructures is aided by these algorithms' ability to sift through mountains of data, adjust to novel dangers, and show impressive precision in detecting hostile actions [18] [19]. By encrypting data and increasing information literacy levels for cloud re-appropriation, AI-based systems like neural networks and anomaly detection algorithms improve cloud security. In sum, the study highlights the promise of AI and ML for improving cloud security and stresses the need for ongoing innovation in creating stronger security measures for cloud computing.

3. Method

According to the study's approach, both qualitative and quantitative methods will be used to present the outcomes, with the aim of being responsive to the data.

Quantitative Analysis:

1. Statistical Tools: Due to rich numerical data, SPSS will be used in analyzing numerical data using various statistical means.
2. Descriptive Statistics: This is how the means, medians, and standard deviations, among other data properties that may be deemed significant in the study, will be summarized and described.
3. Correlation Analysis: This will reveal correlation and co-occurrence between similar and different variables, for example, how the use of AI affects the level of security.
4. Factor Analysis will be used to identify variables that may be causing the trends identified in the data set. This could include analyzing the occurrence of various AI tools and the extent to which AI is believed to be efficient in preventing cyber issues.

Qualitative Analysis:

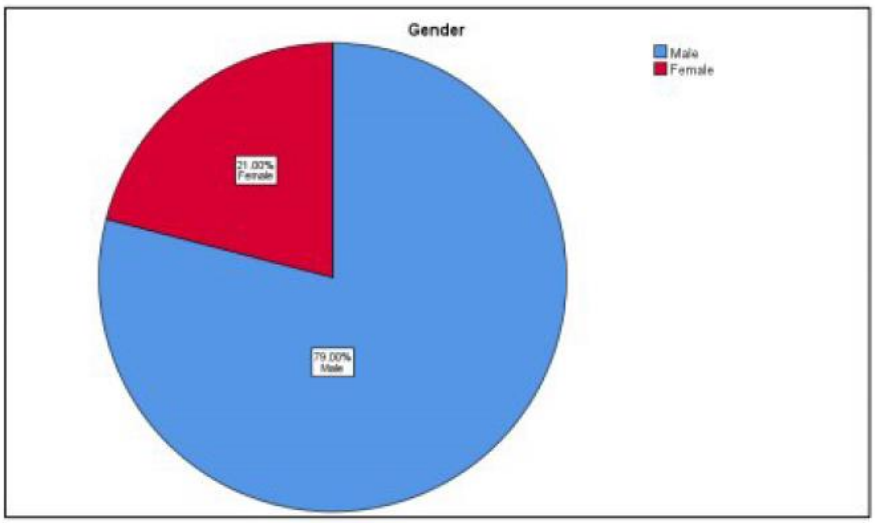
1. Theme Analysis: The interviews will be transcribed to look for a theoretical pattern that may emerge.

2. Detailed Explanation: This analysis will offer a better understanding of the state of affairs in AI's qualitative cybersecurity factors, such as common issues, values, and perceptions within specific sectors.
3. Expert Perspectives: Industry specialists' opinions will allow for identifying the subtleties of AI's application and real-life applications in cybersecurity.

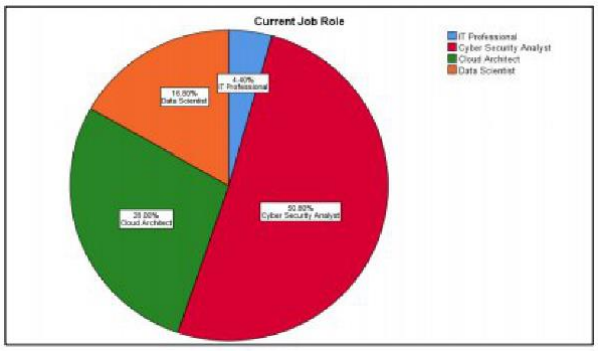
Combining these analyses will offer a comprehensive view of both the statistical trends and the qualitative insights into the effectiveness and challenges of AI in cybersecurity.

4. Results

In a study of 500 participants, 79% were male, and 21% were female, highlighting a significant male dominance among SOC team members in the Indian IT industry.



The study sample of 500 participants includes 4.4% IT Professionals, 50.8% Cyber Security Analysts, 28.0% Cloud Architects, and 16.8% Data Scientists. Over half of the participants are Cyber Security Analysts, reflecting the study's focus on cybersecurity. Cloud Architects and Data Scientists are also significantly represented, making up 28.0% and 16.8% of the sample. Though the smallest group, IT Professionals account for 4.4% of the respondents. This distribution provides a balanced view of the professional roles in AI and cybersecurity within the Indian IT industry.



Among the 500 respondents, 79.6% reported being very familiar with AI in cybersecurity on cloud platforms within the Indian IT industry. Additionally, 14.0% identified as familiar, and 6.4% remained neutral. This data shows that a significant majority of participants are familiar with the topic, indicating that the survey responses are likely informed and relevant. The cumulative percentage reveals that 93.6% of respondents have at least some familiarity, leaving only 6.4% neutral, ensuring a strong foundation for the validity of the study's findings.

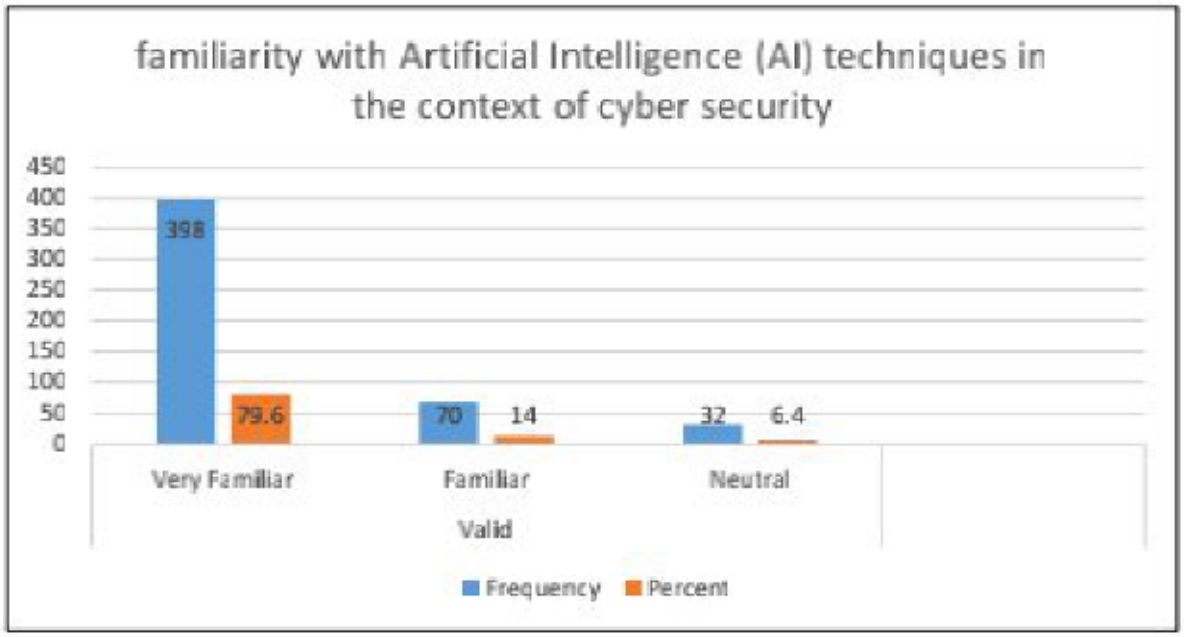


Figure Shows familiarity with Artificial Intelligence (Al) techniques in the context of cyber security.

Among the 500 respondents, 40.0% identified data breaches as the most significant cybersecurity risk, while 20.8% pointed to phishing attacks. 19.0% recognized denial of Service (DoS) attacks as a major risk, and 15.6% cited malware attacks. Insider threats were considered the least prominent risk, with only 4.6% highlighting them. This distribution indicates that data breaches and phishing attacks are perceived as the most critical threats in cybersecurity, with varying levels of concern for other risks.

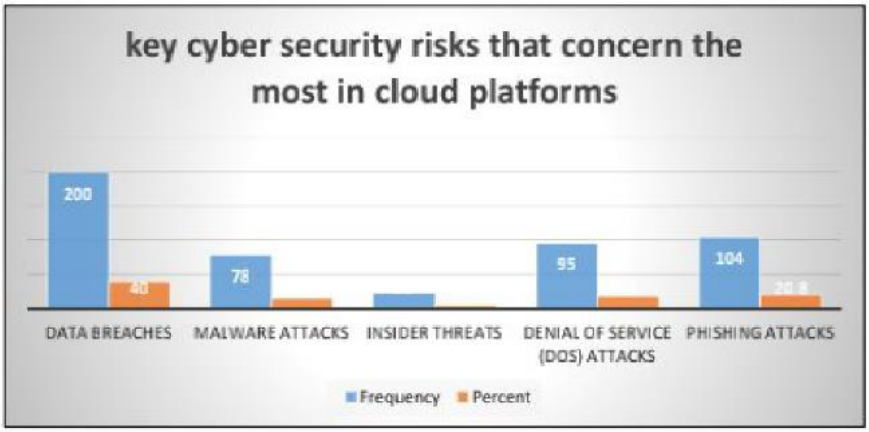


Figure Shown key cyber security risk that concern the most in cloud platforms.

The survey results on the impact of AI-based cybersecurity solutions on the frequency of cyber threats show diverse opinions. 33.6% of respondents observed increased threat frequency despite implementing AI-based solutions. In contrast, 26.6% reported decreased threats, and 24.4% felt the threat level remained unchanged. Additionally, 15.4% noted no change in threat frequency. These findings indicate varied experiences with AI's effectiveness in altering threat dynamics in cloud environments.

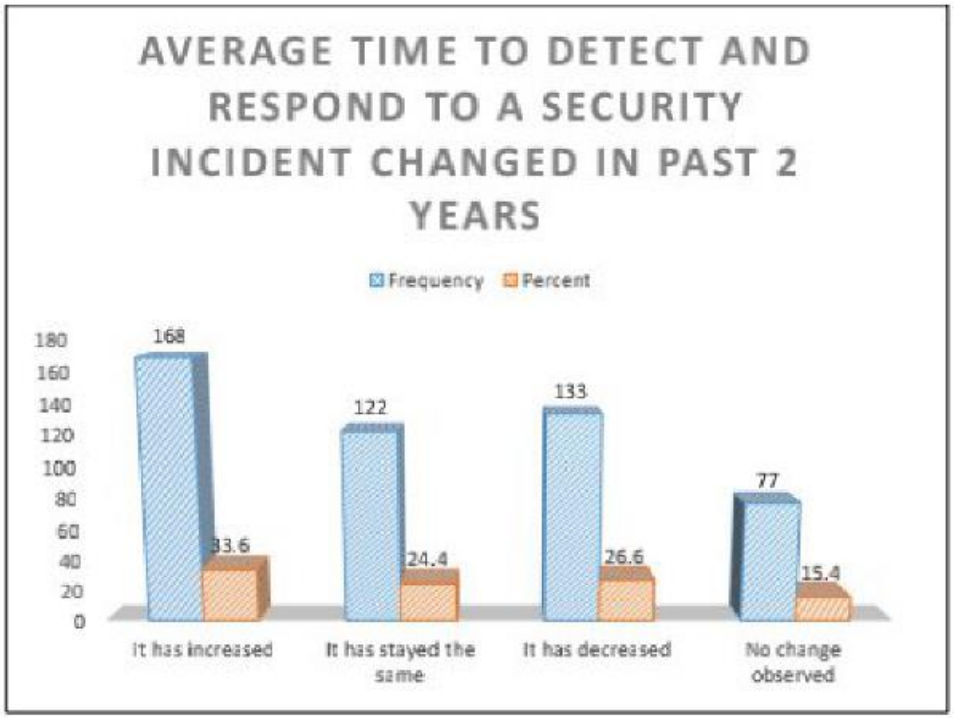


Figure Shows the average time to detect and respond to a security incident changed in the past two years.

The data reveals how respondents assess the effectiveness of their AI-based cybersecurity solutions in managing security threats. A significant 33.2% estimate that these solutions handle 45% of the threats, while 28.4% believe the coverage is around 55%. Additionally, 25% of respondents think the solutions address 49% of threats, and 13.4% report a coverage of 60%. This distribution indicates general confidence in the effectiveness of AI tools but also highlights varying satisfaction levels and potential areas for improvement in threat management.

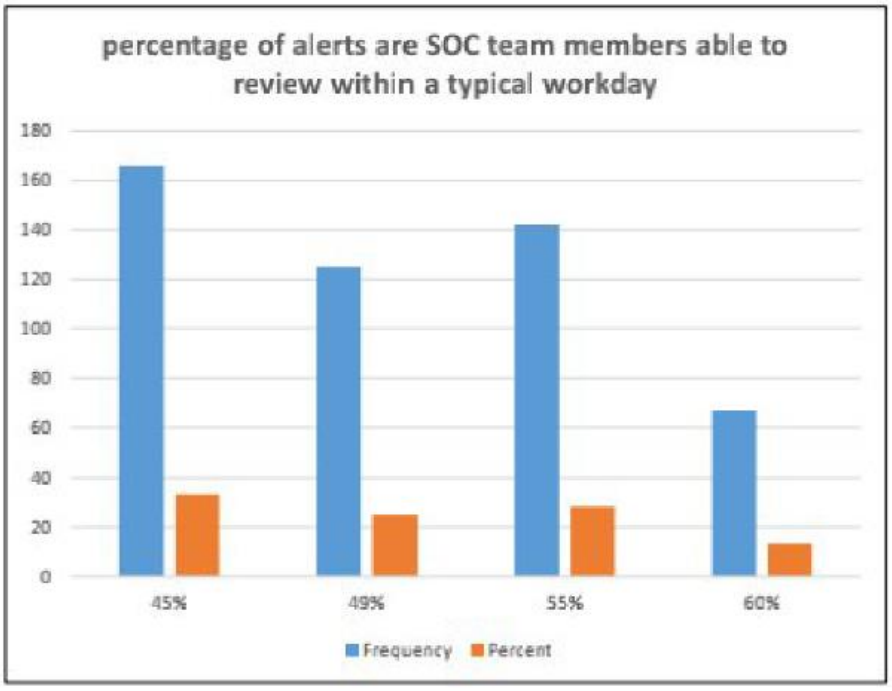


Figure Shown percentage of alerts are SOC team members able to review within a typical workday.

This analysis underscores that the respondents are knowledgeable and well-versed in AI's role in cybersecurity, with diverse experiences and opinions. It indicates that while there is substantial investment in and adoption of AI-based cybersecurity solutions, challenges remain, particularly concerning data privacy and the complexity of integrating these tools. Despite these challenges, there is a clear emphasis on enhancing threat detection and response through advanced AI tools and automation. This points to the fact that, despite the fact

that AI is currently embraced and appreciated for its possibilities, continual work is and ought to be done to grapple with the problems connected with it.

5. Challenges in Cloud Computing

1) Network connectivity: Good network connection is critical for cloud-based applications of ML; functions that involve use of ML algorithms are significantly affected by instances of poor network connectivity. Besides, the synchronization of data with the cloud for further processing is a process in itself, which takes time. The massive time gap when passing data to the cloud does not allow for a timely response and fast actions that, for instance, resolutions require.
2) Data privacy: Security of the information that is shared with machines using the AI cloud computational approach is a significant consideration. Yes, it is as a matter of fact, the confidentiality of personal data. Data collected by AI sensors that are transmitted and processed also comprise of vendors' information as well as customers. Lack of security measures in using the cloud computing on the Web and the mobile platforms could even magnify the existing security threats from data breaches.
3) Security issues: Issues related to security: the issue of security especially on data stored in the cloud is a major challenge:

- Protection of data
- Control of identities and access
- Administration of keys
- Protection of virtual machines

Data security and integrity are the most challenging of the four primary cloud security concerns restricting cloud computing's deployment. Some of these issues are: Managing of key and access; There are some difficulties in using the cloud computing to fulfill data security requirements and these difficulties are CIAT, the abbreviation for Confidentiality, Integrity, Availability, and Traceability.

6. Conclusion

This comprehensive analysis of AI's role in enhancing cloud security within the Indian IT industry reveals significant findings about its impact and effectiveness. The quantitative analysis shows varying levels of AI tool effectiveness, with a substantial portion of respondents perceiving increased threat coverage and others noting limitations or unchanged threat levels. These results, therefore, highlight and establish the possibilities and difficulties of deploying AI in dealing with cloud security.

Analyzing results using the qualitative research paradigm elucidates more practical lessons and professionals' perceptions about AI-driven solutions. It also introduces familiar themes like the daily fight for data protection and integration challenges. It also looks at potentially profitable results such as highly effective threat identification and prevention.

As with many modern applications, the study reveals that AI delivers great improvements in the cloud security front, although there is still work to fine-tune certain aspects. Both the statistical analysis and professionals' insights provide complementary coverage of AI's existing role and future possibilities for strengthening cybersecurity in the IT industry of India. This approach ensures that the strengths, weaknesses, opportunities and threats are defined regarding AI technologies to ensure its improvement to help in more effective cloud security management in the future.

References

Primary sources:

"Artificial intelligence in Cyber Security Risk on Cloud platforms with reference to Indian IT industry" Thesis submitted by Syed Minhaj ul Hassan Mangalayatan University, Beswan, Aligarh, 2024. Unpublished thesis.

Secondary sources:

[1] Subramanian, E. K., & Tamilselvan, L. (2019). A focus on the future cloud: Machine learning-based cloud security. *Service Oriented Computing and Applications, 13*(3), 237–249. https://doi.org/10.1007/s11761-019-00270-0

[2] Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7

[3] Muralidhara, P. (2017). The evolution of cloud computing security: Addressing emerging threats. *International Journal of Computer Science and Technology, 1*(4), 1–33.

[4] Achar, S. (2022). Adopting artificial intelligence and deep learning techniques in cloud computing for operational efficiency. *International Journal of Information and Communication Engineering, 16*(12), 567–572.

[5] Nassif, A. B., Abu Talib, M., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: A systematic review. *IEEE Access: Practical Innovations, Open Solutions, 9*, 20717–

20735. https://doi.org/10.1109/ACCESS.2021.3054129

[6] Khorshed, M. T. (2011). Trust issues create threats for cyber-attacks in cloud computing. In *2011 IEEE 17th International Conference on Parallel and Distributed Systems* (pp. 900-905). IEEE. https://doi.org/10.1109/ICPADS.2011.156

[7] Kumar, R., Lal, S. P., & Sharma, A. (2016). Detecting denial of service attacks in the cloud. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing* (pp. 309–316). IEEE. https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2016.70

[8] Moreno-Vozmediano, R., Montero, R. S., Huedo, E., & Llorente, I. M. (2019). Efficient resource provisioning for elastic cloud services based on machine learning techniques. *Journal of Cloud Computing (Heidelberg, Germany), 8*(1), 1–18. https://doi.org/10.1186/s13677-019-0128-9

[9] Dave, D., Meruliya, N., Gajjar, T. D., Ghoda, G. T., Parekh, D. H., & Sridaran, R. (2018). Cloud security issues and challenges. In *Big Data Analytics: Proceedings of CSI 2015* (pp. 499-514). Springer Singapore. https://doi.org/10.1007/978-981-10-6620-7_48

[10] Nenvani, G., & Gupta, H. (2016). A survey on attack detection on cloud using supervised learning techniques. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-5). IEEE. https://doi.org/10.1109/CDAN.2016.7570872

[11] Hesamifard, E., Takabi, H., Ghasemi, M., & Jones, C. (2017). Privacy-preserving machine learning in the cloud. In *Proceedings of the 2017 on Cloud Computing Security Workshop* (pp. 39–43). ACM. https://doi.org/10.1145/3140649.3140655

[12] He, Z., Zhang, T., & Lee, R. B. (2017). Machine learning-based DDoS attack detection from the source side in the cloud. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 114-120). IEEE. https://doi.org/10.1109/CSCloud.2017.58

[13] Butt, U. A., Mehmood, M., Syed, B. H. S., Amin, R., Shaukat, M. W., Raza, S. M., Suh, D. Y., & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics (Basel), 9*(9), 1379. https://doi.org/10.3390/electronics9091379

[14] 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. https://doi.org/10.1109/CSCloud.2017.15

[15] Malaiyappan, J. N. A., Karamthulla, M. J., & Tadimarri, A. (2023). Towards autonomous infrastructure management: A survey of AI-driven approaches in platform engineering. *Journal of Knowledge Learning and Science Technology, 2*(2), 303-314.

[16] Talati, D. (2023). AI in the healthcare domain. *Journal of Knowledge Learning and Science Technology, 2*(3), 256–262.

[17] Talati, D. (2023). Telemedicine and AI in remote patient monitoring. *Journal of Knowledge Learning and Science Technology, 2*(3), 254–255.

[18] Talati, D. (2024). Virtual health assistance–AI-based. *Authorea Preprints*.

[19] Talati, D. (2023). Artificial intelligence (AI) in mental health diagnosis and treatment. *Journal of Knowledge Learning and Science Technology, 2*(3), 251–253.