International Journal of Engineering and Science Invention (IJESI)
ISSN (Online): 2319-6734, ISSN (Print): 2319-6726
www.ijesi.org ||Volume 15 Issue 4 April 2026 || PP 64-70

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

Yogendra Kumar Vishwakarma[1], Waseem Ahmad[2]
[1]*M.Tech Scholar, Department of Computer Science & Engineering*
[2]*Associate Professor, Department of Computer Science & Engineering*
Vishveshwarya Group of Institutions, Gautam Buddh Nagar

Abstract: *Artificial intelligence in the cloud is a growing field with the potential to revolutionise many industries with its intelligent solutions. The Machine Intelligence and Statistics features of AI clouds allow enterprises to create dynamic applications capable of performing complicated calculations. A company's bottom line or lifespan may be greatly enhanced by creativity (AI) in cloud computing, which focuses on developing intelligent applications, helping companies with big data, enhancing apps via creative algorithms, and predicting and foreseeing success. This article explores artificial intelligence (AI) in the cloud from its inception to its present day, tracking its evolution, pros and cons, trends in the market, applications, and future forecasts.*

Keywords*: The following terms are associated with the analytical framework: cloud computing, AI, ML, IoT, Tesla, algorithms, logistic regression, autonomous ML, data processing, simulated data, and ML.*

I. Introduction

Keeping the data and systems secure should be an enterprise's number one concern in this era of ever-increasing personal data and pervasive cloud technology. The allure of online computing has caused a sea change in company processes and data governance due to its capacity, availability, and affordability. But this convenience isn't without its hazards. To combat the dynamic nature of cyber-attacks, cutting-edge technology that can adjust and fortify cloud security is constantly required. When faced with increasingly complicated threats, standard security methods are necessary, albeit they are efficient to a certain extent. At the intersection of technological expertise lies the solution. Cloud safety is currently headed by AI and ML because of their superior data-sifting, trend-spotting, and decision-making capabilities in real-time. Given the dynamic nature of digital dangers and the limitations of current security measures, our goal is to explore how artificial intelligence and machine learning may transform cloud safety. Our goal is to help cyber security experts and business leaders realise the importance of safeguarding online resources in the modern data-driven era by examining real-world examples and delving into potential future challenges. Join us in this week's episode to learn how AI and other tech-driven solutions can protect cloud users' data from cybercriminals.

Because of the explosion of electronic data and the pervasiveness of cloud computing, information and system safety has risen to the status of a top priority for modern businesses. The use of clouds has really revolutionised the way businesses handle data and operations by opening up new options for scalability, access, and cost cooperation. The downsides of this convenience, meanwhile, are serious and should not be ignored, Samar (2006). In any ever-changing security landscape, the ability to think creatively and devise new ways to fortify the cloud's standing is vital. While older safeguards did have some similarities with today's design, they varied significantly. There is never an answer at the intersection of the mind and the hand. Because of their speed, accuracy, and ability to process massive amounts of data, AI and ML have become more popular in cloud safety. After reviewing the evolution of digital dangers and how conventional security measures have failed, this study moves on to investigate the cutting-edge possibilities presented by AI and MS in securing cloud systems. As a result, this study will center on how current technologies might be used to address future concerns, with the goal of better preparing hackers and executives to safeguard digital resources. Come with us as we explore the murky depths of security and emerge with a future where technological and artificial intelligence guard the cloud's entrance.

II. Literature Review

New standards for safeguarding the cloud, developed by Subramanian E. K., and Latha and Tamilselvan [1], will center on proposed a novel approach that makes use of ML, known as Convolutional Neural Networks ((CNN), to handle and respond to certain situations.

In addition to reviewing research on assaults, threats, and weaknesses in cloud safety, Martins [2] offers a useful method for classifying such traits.
Pavan [3] sheds light on the muralidhara - computing safety structure, discussing emerging dangers and their remedies, with the goal of securing websites and personal information.
The use of the cloud platforms driven by AI are explored in depth by Achar and Sandesh [4]. This includes an examination of their many forms, functionalities, present advancements, and issues.
Nassif [5] investigates potential uses of AI techniques for detecting and preventing cloud safety vulnerabilities.
Two primary contributions are provided by Khorshed [6]: first, a comprehensive review of cloud technology that addresses adoption barriers and issues with threat mitigating; and second, novel concepts for addressing common vectors of attack via the use of creative ML.
Kumar, Raneel,, Sunil Pranit & Lal, and Alok Chandra [7] provide a way to safeguard VMs (virtual machines) hosted in clouds regarding denial-of-service (DoS) attacks.
Moreno-Vozmediano presents and assesses [8] a novel predicting self-scaling technique that makes use of artificial intelligence techniques for time series prediction and creative queue theory.
Cloud safety concerns, such as threats to cloud simulations and network design, are highlighted in research by Dave et al. [9]. These problems affect many sectors that deal with clouds.
This a cloud-based layer is heavily highlighted in the study of creative cloud computing privacy by Nenvani, Geetanjali, and Huma Gupta [10]. Problems with virtualisation, such as unauthorised access to shared images, breaches in solitude, unsafe migrations, and VM escapes, are discussed in this article. Additionally, it delves deeply into IaaS weaknesses and suggests solutions.
Secure protected projections and their secure transfer are made feasible by the study conducted by Hesamifard et al. [11], which demonstrates that educating neural networks with creativity using protected data is not only feasible but also feasible.
He, Zhang, and Lee [12] present a technique for identifying cloud-based denial-of- service threats via the use of generative creative ML techniques.

Butt and associates [13] offer an in-depth examination of cloud security concerns, issues, and fixes using a variety of training approaches, including supervised learning, semi-supervised learning, supervised learning, and reinforcement learning.
The scientists in Mansour and [14] examine outlier detection and categorisation, which goes against the grain of modern study methodology.
Boosting detection tools for intrusions and ensuring the security of cloud data requires the use of AI and machine learning. Multiple articles have emphasised the use of machine learning techniques, including supported vector machine, XGBoost, AI, a randomised forest, and ensemble learning for cloud cyber threat identification and mitigation [15, 16, 17]. Computers like this help keep clouds secure by sorting through massive amounts of data, adapting to new threats, and identifying hostile behaviours with remarkable accuracy [18] [19]. Artificial intelligence (AI) solutions, such as brain networks and detecting anomalies methods, enhance cloud safety by storing data and raising knowledge levels to prevent cloud stealing. All things considered, the research shows that AI and ML have great potential to make safety in the cloud better, and it emphasises the need of constant creativity in this area.

III.Method

In order to respond to the data, the research will employ a combination of qualitative and quantitative techniques to communicate the findings, as per its strategy.

Quantitative Analysis:

1. Statistical Tools: Because there is a lot of data in numbers, SPSS will be utilised to analyse it statistically.
2. Descriptive statistics: This is where the analysis's important data features, such as means, averages, and variances, will be summarised and explained.
3. Thirdly, we have creative correlation, which will show us how related and distinct aspects are, as well as how they interact, for instance, how AI impacts safety.
4. The statistics set's tendencies will be investigated utilising factors to uncover potential causes. This can involve looking at how often different AI technologies are used and how effective people think AI is at avoiding cyber problems.

Qualitative Analysis:

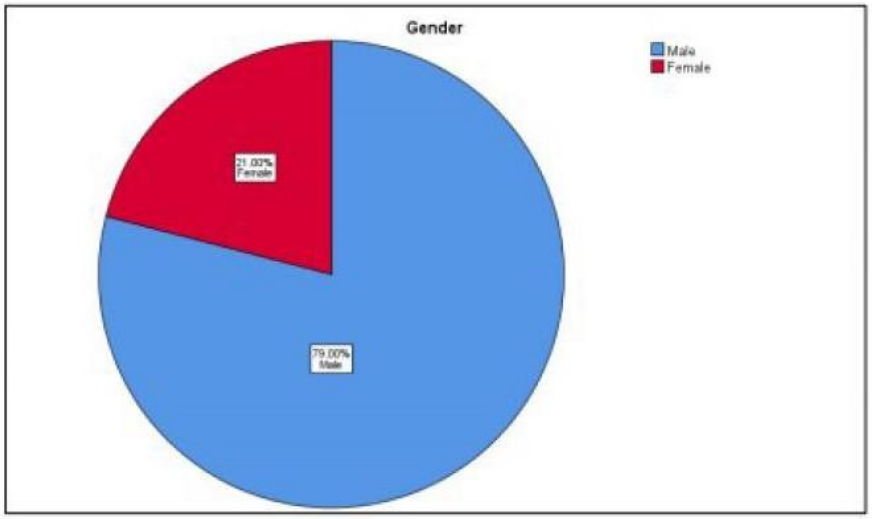
1. Theme Analysis: An abstract structure will be sought by transcribing conversations.
2. Detailed Explanation: By breaking out AI's subjective insecurity factors—like industry-specific norms, attitudes, and perspectives—this study will provide light on the current situation.

3. Expert Perspectives: The comments of experts in the field will help us understand the nuances of AI as its practical uses in cybercrime.

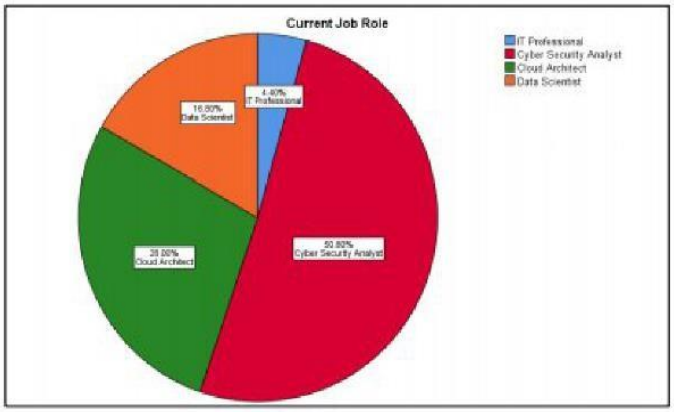
By integrating various studies, we can see the big picture of the analytical tendencies and qualitative hints into the pros and cons of AI in defence.

IV. Results

A research conducted in the Indian IT sector found that out of 500 people surveyed, 79% are male and 21% were female. This suggests that there is a notable gender parity among SOC colleagues.

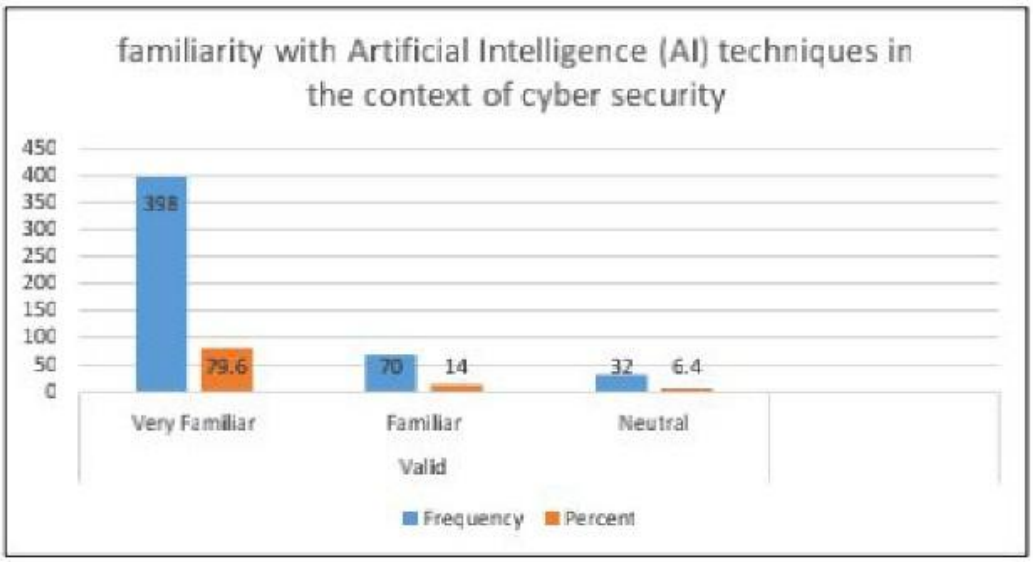


Information technology specialists make up 4.4% of the 500 people surveyed, whereas technology experts account for 50.8%, cloud designers for 28.0%, and data researchers for 16.8%. Analysts in security make up more than half of the subjects, indicating that this is a research focused on protection. There is a sizable contingent of cloud architecture and data engineers as well, which making up 28.0% and 16.8% of the sample, respectively. Information Technology Specialists make up the lowest subset of participants (4.4%). This breakdown offers a fair representation of the many job functions in the Indian IT sector related to artificial intelligence and terrorism.



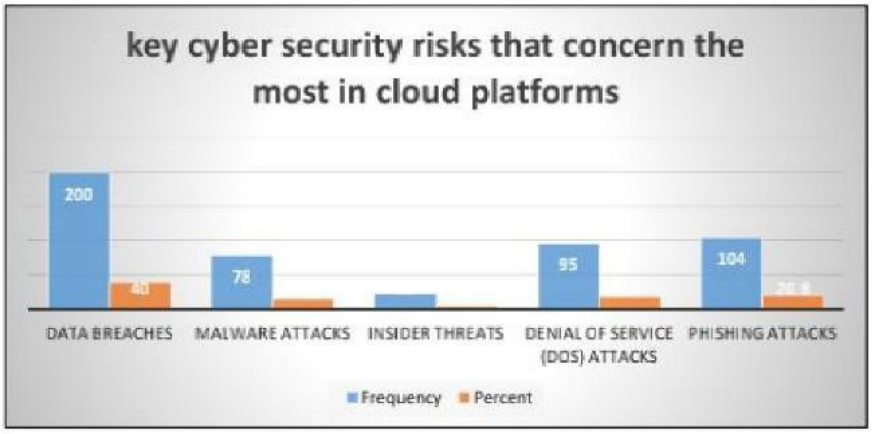
For the Indian IT sector, 79.6% of the 500 participants were extremely knowledgeable about AI in protection on cloud-based systems. There were also 14.0% who said they were aware and 6.4% who said they weren't sure. Based on these results, it seems that most people who took the poll had some background knowledge on the subject.

answers are probably well-informed and applicable. With 93.6% of participants having some acquaintance and 6.4% being impartial, the research's findings may be confidently said to be based on solid evidence.

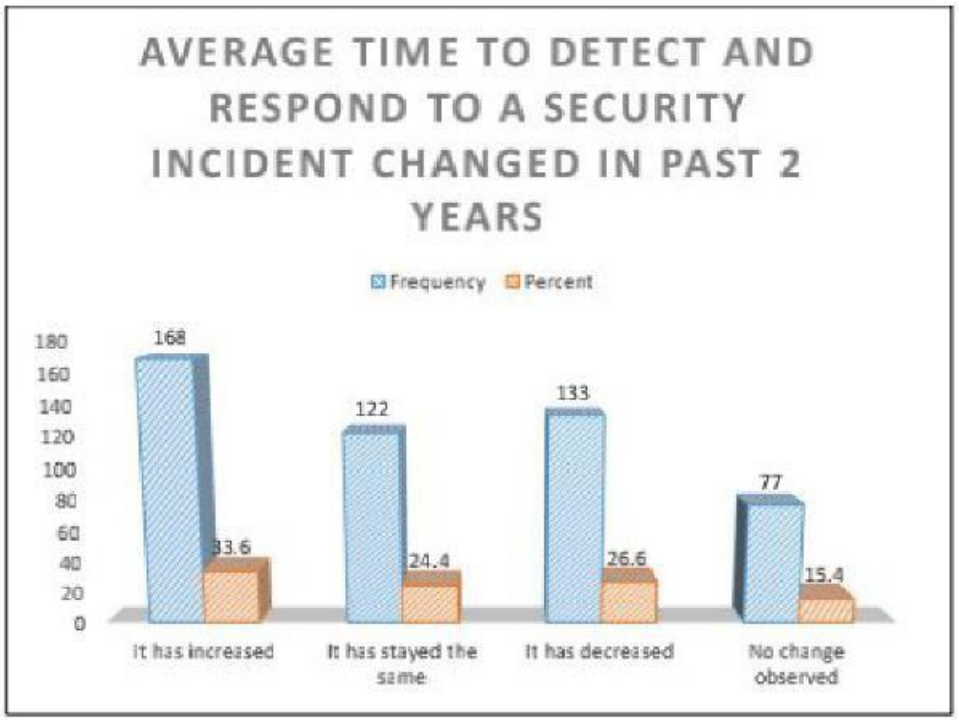


Knowledge of AI methods as they pertain to cyber protection is shown in the one shown.
Out of 500 people surveyed, 40.0% said that data intrusions were the biggest cyber danger, while 20.8% said that phishing scams were the worst. One-ninth of the people saw DoS assaults as a big threat, and

Threats from spyware were mentioned by 15.6% of the participants. Only 4.6% of respondents ranked threats from inside as a high priority. According to this shipment, different people are worried about different security concerns, but the majority think knowledge leaks and phishing attempts are the biggest problems.

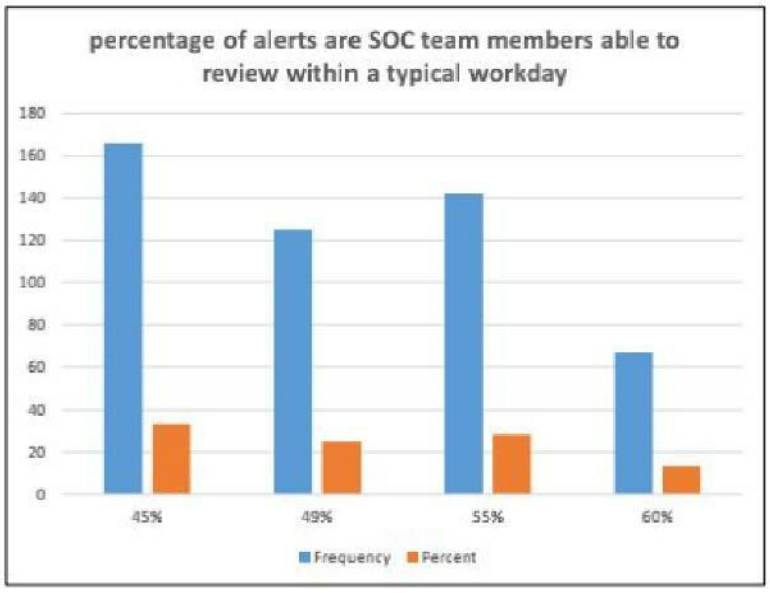


The most important cyber security risks associated with cloud-based services are shown in Figure.
Attitudes vary according to the poll findings about the effect of safety measures using AI on the number of hackers. The majority of responders (33.6%) saw a reduction in danger severity even after using AI- focused on answers. On the other hand, although 24.4% thought the level of danger was the same, 26.6% said it had dropped. Further, 15.4% said that the regularity of threats remained unchanged. These results show that people have different opinions on how well AI changes threat behaviours in cloud settings.



It displays the shift over two years ago in how long it takes to identify and react to a safety concern.
Data shows how those polled rate the efficacy of the security measures that use AI for threat management. A substantial 33.2% believe that these remedies address 45 percent of the dangers, while

Regarding the protection, 28.4% think it's close to 55%. Further, 13.5 percent of people say the remedies cover 60 percent of dangers, and 25 percent say they cover 49%. While this range does show that people are generally confident in AI technologies' performance, it also shows that people aren't all satisfied and that risk mitigation may be better.



See Figure for the breakdown of the alerts that people of the SOC team may usually assess in a day.
The results show that those polled had a wide range of tales and views on the topic of artificial intelligence's function in safety. While there is a lot of money going into and integration of these technologies and concerns about privacy of data still as obstacles to the widespread use of AI-driven security measures. Notwithstanding these obstacles, the use of sophisticated AI techniques and automating to improve threat identification and reaction is a top priority. It is evident from this or that, even

Since AI is being welcomed and valued for its potential, there has to be ongoing effort to address the issues related to it.

V. Challenges in Cloud Computing

1) First, you need an accurate network link if you want to employ machine learning (ML) in the cloud. When this isn't the case, anything that relies on ML methods will suffer greatly. Furthermore, data synchronisation with a cloud platform for further analysis is an independent operation that also requires time. Timely responses and quick actions are required for things like decisions, but they are not possible because to the enormous time difference when content is sent to cloud services.

2) 2) Data privacy: A major factor to think about is the protection of knowledge that is transmitted with computers when employing the AI cloud computing technique. In truth, it is the privacy of individual records. Data supplied and analysed by AI devices also includes data regarding suppliers and consumers. Even more serious than current safety hazards from information theft are the lack of safeguards when working with cloud services on smartphones and the Internet.

3) Concerns with assurance: Concerns about safety: a big obstacle is the problem of safety, particularly with regard to data kept on the the internet:

- Keeping information safe
- Identity and permission control
- Managing access credentials
- Keeping virtual computers safe

Using the 4 main safety concerns that limit the development of the cloud, information safety and integrity provide the greatest challenge. Here are a few of these problems: The use of clouds presents a number of challenges when it comes to meeting privacy standards, including key and access management, CIAT (Principality, Excellence, Accessibility, and traceability),, and so on.

VI. Conclusion

The effects and efficacy of artificial intelligence (AI) in strengthening cloud safety in India's IT sector are uncovered in this extensive study. Analytical investigation reveals mixed results about the efficacy of AI tools; whereas a few people saw expanded concern detection, others saw restrictions or no shift in danger rates. Consequently, our findings demonstrate the potential and challenges of using AI to address cloud safety.

Results analysed employing a qualitative approach provide light on experts' views on AI-driven approaches and additional valuable insights. It also brings up old ground, such as the never-ending struggle for security of data and integrating hurdles. Monetary outcomes, such efficient threat detection and avoidance, are also considered.

The research confirms that AI, like many other contemporary technologies, greatly enhances safety in the cloud, while certain parts still need fine-tuning. The current and possible future roles of AI in enhancing safety in the IT sector in India may be better understood with the use of mixed statistical techniques and expert opinions. To better manage cloud safety in the years to come, this method defines the SWOT of AI innovations, which stands for advantages, disadvantages, potential, and dangers.

References Primary sources:

"The Role of Using AI in Assessing Cyber Safety Risk on Cloud Computing Services: A Case Study of the Indian IT Market" (Syed Muhammad ul Hassan,. MBA, Mangalayatan IT Institute of Technology, Beswan, Aligarh, 2024). Thesis not yet available.

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.