International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

AI-Infused Threat Detection and Incident Response in Cloud Security

Sumanth Tatineni

Devops Engineer, idexcel Inc
Email: *sumanthtatineni.ts[at]gmail.com*

Abstract: ***With the evolving sophisticated attack techniques and cyber-attacks, businesses must adapt their threat detection and response mechanisms. It is paramount to explorecontemporary tools, from real-time monitoring and network forensics to XDR,SIEM, SOAR, and NDR, giving insights into the ever-changing detection and response systems space. The migration of business data and applications to the cloud has dramatically improved security and threat detection. Conventional security approaches must be revised to guard against advanced threats within the fragile network infrastructures of cloud environments. By understanding this challenge, artificial intelligence (AI) comes in to help enhance the accuracy and speed of threat response and identification. This paper depicts the impact of AI on cloud security and threat detection. As cyber threats increasingly target service providers and cloud infrastructures, the demand for robust, easily deployable security measures remains essential. To address this issue, this paper will address the collaboration between cloud security and AI operations, stressing the resultant acceleration in incident response times – further depicting how this relationship strengthens an organization's defenses and curbs the impact of security incidents. For organizations looking to keep up with the dynamic threat landscape, leveraging and understanding the relationship between cloud security and AI is essential in maintaining an adaptive and resilient security posture.***

Keywords: AI-driven threat detection, real-time monitoring, data protection, incident response, cloud security solutions, cloud infrastructure, threat detection

1. Introduction

The prevalent adoption of cloud technology continues to reshape the digital space, with 39% of organizations hosting over half of their workloads on cloud platforms [1]. The massive surge in multi-cloud usage further depicts this shift towards the cloud, as about 69% of organizations embrace two or more cloud service providers, with companies such as Amazon Web Services and Microsoft Azure leading. Nonetheless, this substantial migration causes concerns, particularly regarding data security within these dynamic cloud spaces [2]. Amidst the dynamic threat landscape of 2023, it is essential to have a proactive approach to cloud security. Cyber security professionals are concerned about threats such as insecure interfaces/APIs, misconfigurations, DDoS attacks, and unauthorized access.

Additionally, Internet of Things (IoT) technologies introduce vast amounts of data and attack surfaces that demand proper safeguarding to curb potential exploits [3]. With this complex security space, incident response becomes a central concern in an organization's defense strategy, being the initial fortification against threats and providing groundwork for future risk mitigation [4]. Integrating AI into the IR process is a transformative shift, streamlining resolution efforts with unmatched efficiency, speed, and human effort. Organizations can quickly detect, comprehend, and mitigate threats by automating the incident response with AI [5]. The merits of infusing AI into incident response are clear – with AI taking on the role of data analysis and monitoring, human analysts are left to concentrate on more important things that require human expertise and judgment. This article delved into the relationship between AI-driven incident response and cloud security [6], looking at how the fusion strengthens the organization against evolving threats and empowers cyber security teams to navigate the challenges brought about by today's digital space.

2. Background and significance of AI-infused threat detection and incident response in cloud security

As organizations increasingly move their applications and data to the cloud, the need for advanced threat detection and efficient incident response becomes more important. AI integration into cloud security operations is the solution to address the challenges cyber threats bring. This paper looks into security technology, delving into AI-infused approaches beyond traditional methods. As cyber threats arise, organizations need to adopt advanced and innovative measures to safeguard sensitive data hosted in the cloud.

AI facilitates more accurate and faster incident response. To minimize the impact of security incidents, timelines are crucial in response, and AI automation ensures quick actions, thus reducing manual response time and interventions. Therefore, understanding the strategic merger between cloud security and AI operations mitigates the damage from security incidents, which is relevant information for organizations looking to be on the lead with these threats. The paper aims to recognize the persistent and immediate demand for strong security measures for the highly targeted cloud infrastructure and help organizations develop effective and targeted security solutions.

2.1. How AI is used in threat detection

Identifying potential threats in cloud security is vital in maintaining a solid defense against cyber threats. AI introduces advanced capabilities beyond the usual traditional techniques to help organizations bolster their security [7].

Here is how AI empowers proactive threat identification in cloud security;

2.1.1. Anomaly detection

In anomaly detection, AI systems thrive in uncovering deviations from normal behavior, thus providing an essential defense against zero-day attacks. This approach stands on the establishment of baselines, which is a dynamic process where AI continuously learns and monitors from the complex web of user and system activities within a cloud environment [8]. AI's anomaly capabilities start with the proper establishment of baselines that incorporate what involves normal activity within the cloud ecosystem. Through continuous observation and learning, AI can discern the typical interactions and patterns among applications, systems, and users. A thorough understanding allows for identifying deviations that may depict potential security threats quickly.

Additionally, the user behaviors, network activities, and system processes are analyzed continually, thus allowing AI systems to refine and adapt their understanding of what is known as normal, thus ensuring that the baselines remain relevant in case of changing system configurations and user patterns [9]. Once the baselines are established, AI becomes an expert at quickly identifying anomalies – the unexpected deviations from learned norms. Note that anomalies can take different forms, from atypical data transfers to unusual access patterns. The quickness of AI-driven anomaly detection is important as it allows the quick identification of potential threats like zero-day attacks, which were traditional techniques used but would have failed. Therefore, by learning and adapting to normal behavior, AI systems can flag deviations that align with the attributes of zero-day attacks, for example, abnormal system behavior, unexpected data access, or unusual network traffic, which can be indicators to signal a potential threat.

2.1.2. Behavioral analytics

AI can detect and assess suspicious activities to strengthen defenses against insider threats regarding behavioral analytics and user monitoring. This approach depends on AI's aptitude for learning normal user behavior and strictly identifies deviations from established norms. AI seamlessly includes behavioral analytics into cloud security through User and Entity Behavior Analysis (UEBA). By properly assessing the actions and behaviors of users and entities within the cloud environments, AI is keen on identifying activities that deviate from the established norms [10]. For example, AI can discern whether or not a user is trying to access sensitive data from an unauthorized location, thus providing a proactive defense against unauthorized access.

The major challenge in cyber security is detecting anomalies with the huge streams of system and network events. Therefore, due to exhaustion or boredom, AI tools thrived in giving attention to event data streams. Behavioral Threat Analytics (BTA), or User and Entity Behavioral Analytics (UEBA), deals with individual actors' event streams that analyze unusual environmental behavior and examine how specific systems or individuals behave in certain contexts [11]. Establishing profiles of normal behavior for users, AI within cloud security can strictly detect anomalous activities depicting compromised accounts or any insider threats. This analysis considers accessed resources, data download patterns, geo-locations, and login timing. In addition, natural language processing allows AI to scan communications for signs of potential threats.

2.1.3. Automated incident response

AI streamlines incident handling processes, thus minimizing damage and expediting recovery times. AI can do this through its capacity to quickly identify and respond to threats without requiring human intervention. This aspect of security automation enhances the efficiency of incident response and allows for seamless and advanced threat detection and response in cloud security. The quick identification and response to threats with AI minimize the impact of security incidents without depending on manual intervention. For example, AI can automatically quarantine infected devices or revert changes made by cyber criminals, thus ensuring a quick and efficient response to emerging threats.

Additionally, security automation covers an array of repetitive and mundane security tasks prone to human oversight. These include configuring firewalls, conducting malware scans, responding to alerts, patching vulnerabilities, and executing password resets [12]. When these security tasks are automated using AI, the cyber security teams are freed from routine activities, and this empowers them to focus on higher-value tasks such as threat hunting, continuous monitoring, and refining the overall security state. When the teams are relieved of these repetitive tasks, AI-driven automation improves response times and reduces the likelihood of errors, thus ensuring a more effective and agile security frame, contributing to continuous security improvement.

2.1.4. Threat intelligence

AI systems help organizations stay ahead of the evolving threat space by integrating with threat intelligence feeds. The integration allows real-time updates, thus ensuring that the cloud security infrastructure is dynamically informed about the latest known threats. Thus, by staying above threat intelligence, AI-infused security measures can help identify and respond to potential risks based on the most up-to-date information. Consequently, AI tools play a huge role in determining optimal encryption strategies within complex cloud environments. The complexity of a distributed cloud ecosystem requires a refined approach to encryption, balancing security and performance consistently.

AI helps by automating key management, selectively encrypting high-risk data, and applying adaptive encryption models curated to specific services and applications. The impending need for post-quantum encryption algorithms leveraging AI highlights the role of advanced technologies in strengthening cloud security against possible threats like quantum computing attacks [14]. With AI being able to process vast amounts of data, it allows for predictive analysis. This is done by learning from known threats. AI can predict and prevent possible threats that may not be identified yet, like forecasting which systems are most likely to be targeted by specific threat actors, thus providing

organizations with actionable insights to strengthen their security defenses promptly.

2.1.5. Cloud-native security tools

Providers offer solutions that integrate AI seamlessly for advanced threat detection and incident response. When explicitly tailored for cloud environments, these tools are essential components to enhance security measures. A cloud-native security platform (CNSP) offers a comprehensive solution for managing security across different clouds from various providers. By creating a security strategy that includes best practices applicable to multiple parties, a CNSP becomes an essential component for simplifying cloud-native monitoring, disaster recovery, and compliance efforts.

Cloud-native solutions merged with AI capabilities provide real-time visibility into cloud activities. This integration pushes organizations to respond to threats immediately, leveraging AI for advanced threat detection and incident response. By utilizing the adaptive attribute of AI, these tools improve the security state in cloud environments, thus dealing with the issues of evolving cyber threats [14]. Therefore, organizations can streamline their security measures across different clouds and providers, thus allowing a standardized and cohesive approach. This strengthens cloud-native monitoring and establishes a strong foundation for disaster recovery and compliance, thus pushing for the resilience of cloud security frameworks.

2.2. The role of AI in modern security

With the shift in modern security, particularly with 45% of breaches being cloud-based and 80% of companies experiencing at least one cloud security incident in the last year, there is no doubt that AI could be the solution [15]. Over the decades, security software has automated routine tasks, reducing the reliance on manual intervention. Yet, analyzing events, identifying anomalies, and connecting diverse data to distinguish genuine security threats from false alerts have primarily remained within the human expertise zone, often with the help of tools. AI use in cybersecurity is posed to change this situation significantly.

The traditional dependence on human attention for complex tasks may find a partial replacement as AI comes in to evaluate events and bring forth relevant responses. In cybersecurity, human attention is the scarcest resource among teams. Cybersecurity professionals often face the challenge of sourcing, training, and retaining skilled staff. AI tools will eradicate this challenge. For instance, a well-executed zero-trust strategy creates an environment where fewer anomalous events are likely to happen, reducing the volume of routine evaluations. AI's intervention allows professionals to focus on high-level assessments and strategic initiatives.

3. Best practices for AI- Infused Cloud Security

To fully unlock the potential of AI in cloud security and threat detection requires adherence to best practices. By adhering to these best practices, organizations can maximize the effectiveness of AI in cloud security, thus ensuring a resilient defense against any security challenges. Here is what organizations need to consider to strengthen their approach;

3.1. Adopt a multi-layered security structure.

Include AI within a multi-layered security framework that covers network segmentation, strict access controls, and other robust security measures. This approach ensures an organization has a comprehensive defense against different cyber threats. Safeguard sensitive information in the cloud by prioritizing encryption [16]. Data should be encrypted both in transit and at rest to prevent unauthorized access. Establish solid key management processes, like regular key rotation and secure storage practices.

3.2. Continuous Analysis

Utilize the power of AI for continuous analysis of cloud environments by assessing the potential threats; AI-driven systems can provide real-time insights with findings related to the system to improve accuracy and overall performance. Additionally, schedule routine vulnerability assessments to know potential weaknesses in your cloud infrastructure [17]. These assessments should be complemented with penetration testing to simulate real-world attacks, thus evaluating the organization's defensive capabilities against threats.

3.3. Integration with existing security tools

Integrate AI-enabled security tools with your existing security infrastructure seamlessly. This integration creates a merged view of the security environment, promoting cohesion between AI-driven capabilities and established security measures. In addition, ensure that, as an organization, the security features and tools offered by the cloud service provider are understood and adhered to [18]. Understanding the shared responsibility model is essential to ensure security obligations are fulfilled. Ensure the native cloud security services are leveraged, such as AWS Security Hub, Azure Center, or Google Cloud Security Command Center, to improve the overall security.

3.4. Deploy advanced security monitoring

Organizations should strengthen their cloud security through continuous monitoring and intrusion detection systems [19]. The continuous surveillance of the cloud environment helps identify potential threats and unusual activities. Additionally, it enhances monitoring capabilities with an AI-powered intrusion detection system for real-time threat analysis. Agent-based technologies that directly interact with the environment provide advantages for automated incident response [20].

3.5. Alert triage with AI

AI for alert triage enhances the effectiveness and efficiency of incident response in cloud security. Alert triage incorporates categorizing and prioritizing security alerts to ensure that the most critical issues are addressed strictly. AI-

powered systems can automatically analyze incoming security alerts, thus assessing the severity and relevance of each alert based on predefined criteria. The automated analysis streamlines the triage process, thus allowing security teams to focus on addressing the most critical threats first. Consequently, machine learning algorithms can offer contextual understanding to security alerts. This way, by considering historical data, user behavior, and the overall security landscape. AI can differentiate between genuine threats and false positives.

Additionally, AI thrives in pattern recognition and anomaly detection, enabling it to identify subtle signs of potential security incidents. This is essential in alert triage, where distinguishing between abnormal and everyday activities is vital for accurate prioritization. AI systems can integrate with threat intelligence feeds, thus enriching the analysis of security alerts with real-time data about known threats. This enhances the accuracy of alert triage by providing a broader context and allowing quick identification of emerging trends [21]. AI systems can learn from past incidents and feedback from security analysts, which helps adapt to evolving threat landscapes, thus reducing response time. Therefore, organizations can customize their triage systems based on their security priorities and policies, ensuring that the process aligns with the unique security needs of each organization. While AI can automate the initial stages of alert triage, human expertise is required to handle complex situations, make judgment calls, and provide insights that AI may fail to capture.

3.6. Automated containment measures

AI systems autonomously execute actions like blocking suspicious IP addresses and quarantining infected devices. Employing automated patch management, quarantine techniques, and threat blocking enables quick responses to security incidents. For example, upon detecting a malware outbreak, AI can isolate infected systems automatically, thus preventing further spread. This could happen by blocking the source IP address and internal systems that are already compromised, thus deploying anti-malware tools or patches before restoring them online. Automated containment actions facilitate quick and precise responses.
While professionals could be notified, AI has already restricted the incident's severity and scope. Analysts can then determine follow-up actions for comprehensive threat remediation. Specific AI platforms provide 'one-click' containment actions, allowing analysts to trigger predefined playbooks for isolating, patching, and blocking when confirming a detection as malicious; this process eliminates manual steps, thus expediting containment [22]. Containment is an important aspect of incident response since it automates and accelerates efforts that are significant advancements for SOCs looking to improve security efficacy and operational efficiency. This AI potential and advanced analytics extend across different stages of the incident response lifecycle.

3.7. Identifying potential vulnerabilities through AI-driven analytics

In integration, AI-driven analytics identifies and addresses potential vulnerabilities. This technique continuously monitors and assesses an organization's IT environment, leveraging algorithms to detect outdated software, misconfigurations, and configuration errors that could create security gaps. The effectiveness of AI analysis is in its ability to correlate data from different sources, providing an in-depth view of the security scope [23]. This view allows for prioritization of critical vulnerabilities, thus empowering security teams to address them before they can be exploited.

Therefore, quickly detecting threats, assessing their severity, and pushing for appropriate responses helps contain threats before they escalate, thus reducing response times and minimizing potential damage.Additionally, AI algorithms assist in threat-hunting activities by flagging suspicious patterns and emphasizing potential threat indicators. AI makes the hunt more straightforward and more effective in identifying and neutralizing emerging threats. With analytics, organizations can predict potential vulnerabilities and threats, thus empowering them to take preventive measures that strengthen their defenses against evolving threats.

4. Benefits of infusing AI into cloud security

The incorporation of AI into cloud security assessment breeds different benefits. Collectively, they contribute to a more resilient and adaptive cloud security infrastructure, thus addressing the evolving challenges posed by advanced cyber threats in cloud environments.

4.1. Proactive threat detection

Unlike traditional techniques, AI-powered systems can anticipate security threats by analyzing anomalies and patterns within massive datasets. This predictive ability allows organizations to identify potential risks before they escalate further, thus contributing to a more assertive and more anticipatory security posture.

4.2. Real-time responses

AI's real-time capability is essential in strengthening cloud security. The moment a potential threat is identified, AI systems initiate an instant reaction, ensuring a quick and agile response to curb the impact of the threat [24]. This responsiveness is vital in the dynamic space of cloud environments, where quick intervention is needed and time is always essential to maintain the integrity of digital assets.

4.3. Efficient resource allocation

AI's analytical prowess aims to identify optimal resource allocation within cloud security frameworks. AI optimizes security efforts by discerning where security resources are most required, ensuring that resources are deployed strategically to areas with heightened vulnerability. The efficiency allows both overall security and also streamlines resource management.

4.4. False positives reduction

Advanced algorithms used by AI contribute to a considerable reduction in false positives. By fine-tuning the analysis of security incidents, AI minimizes the occurrence of false alarms that can strain security teams [25]. This threat identification precision enables security professionals to focus on genuine concerns, thus improving the overall efficacy of the security system.

4.5. Continuous learning

AI systems can continuously learn since these systems accumulate experience and data; they go through improvement and refinement over time. Regarding cloud security, it translates to AI becoming even more efficient in threat detection and response as it adapts to emergingtactics and patterns used by malicious actors.

4.6. Incident automation opportunities in cloud security

Unlike traditional incident response plans, automated incident response powered by AI can monitor millions of security events effectively daily. This minimizes incident handling time, ensuring threat detection is done quickly, a key component for the efficacy of incident response automation [26]. As cyber-attacks become more prevalent, the manual nature of traditional incident response methodologies can hinder breach detection and response. But with AI technology, security investigations accelerate, thus strengthening organizations against any threats.

- Artificial intelligence allows automated assignment of response duties by suggesting the allocation of engineers during incident response, thus evaluating their availability and expertise based on the nature of the incident [27]. This automated approach improves the deployment of the right resources, thus optimizing the overall response process.
- AI pushes for malware classification and risk analysis by looking over current and historical data, identifying anomalies aimed at regular operations, and signaling potential threats[28]. Machine learning identifies patterns that show malware, thus facilitating risk classification and analysis for informed decision-making.
- Automated incident response seamlessly integrates security protocols into the SDLC from its inception, thus establishing a solid security platform that ensures security measures are deep into the development process [29].
- AI-infused incident response processes provide scalable management of security alerts, thus prioritizing response activities and directing resources to high-stakes tasks [30], improving incident response efficiency and ensuring an organized and focused effort.

5. The future of AI in cloud security

As cloud computing evolves even further, the future of AI in cloud security will continue to witness a transformative shift [31]. Traditional defense mechanisms need to be improved, especially with the cyber threats growing daily. Integrating AI with cloud security is bound to bring more opportunities for organizations and businesses [32]. The future of AI in cloud security will provide a security state where AI technologies respond and detect threats and handle compliance management, risk assessment, and secure development life cycles [33]. Additionally, automation driven by AI algorithms will provide real-time threat detection and immediate actions, thus minimizing the impact of potential breaches.

6. Conclusion

The positive impact of AI integration into cloud security lies in allowing organizations to implement data-driven security strengthened by intelligent automation. In the future, essential technologies such as natural language processing, deep learning, and explainable AI will become even more essential to safeguard the next-generation cloud from evolving threats. Organizations must include AI in their long-term cloud security strategy, creating a new form of predictive, content-aware security by intelligent automation. The potential for AI to transform cyber security is evident through deployment, which empowers organizations to quickly and effectively detect and respond to cyber threats, safeguarding systems, critical data, and networks.

The fast-approaching future of cybersecurity is undoubtedly AI-driven, thus prompting organizations to invest in AI-centric cyber security solutions to stay afloat in the ever-changing landscape. For instance, Microsoft is leveraging AI in its Azure cloud platform to detect and thwart security threats. Google is also using AI to safeguard its cloud customers from phishing attacks, depicting the practical application of AI in enhancing cloud security.

While AI proves to be the solution in cloud security, it is essential to note that it is not a one-size-fits-all solution. A comprehensive approach to cloud security is vital, including different measures like multi-factor authentication, encryption, and regular security audits. However, AI is still a central force in cloud security as it ensures that cloud resources remain accessible only to authorized users, thus playing an important role as reliance on the cloud continues. As the applications and data trajectory align closely with the cloud, AI's importance in enhancing safety is poised to become even more pronounced.

References

[1] Sharma, M., Gupta, R., & Acharya, P. (2023). Adoption and forecasting of technology: modeling the dynamics of cloud adoption using a system approach. *Journal of Enterprise Information Management*.

[2] Ogunde, N. A., &Mehnen, J. (2013). Factors affecting cloud technology adoption: potential user's perspective. In *Cloud Manufacturing: Distributed Computing Technologies for Global and Sustainable Manufacturing* (pp. 77-98). London: Springer London.

[3] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, *11*(2), 198.

[4] Dimitrov, W. (2020). The impact of the advanced technologies over the cyber attacks surface. In *Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-line Conference 2020, Vol. 2 9* (pp. 509-518). Springer International Publishing.

[5] Sarker, I. H., Khan, A. I., Abushark, Y. B., &Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), 296-312.

[6] Vijay, G. S., Sharma, M., & Khanna, R. (2023). Revolutionizing network management with an AI-driven intrusion detection system. *Multidisciplinary Science Journal*, *5*.

[7] Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and preve Kumar, N. (2023). AI in Cybersecurity: Threat Detection and Response with Machine Learning. *TuijinJishu/Journal of Propulsion Technology*, *44*(3), 38-46.ntion. *International Journal of Advanced Engineering Research and Science*, *10*(5).

[8] Samariya, D., & Thakkar, A. (2023). A comprehensive survey of anomaly detection algorithms. *Annals of Data Science*, *10*(3), 829-850.

[9] Alanazi, R., &Aljuhani, A. (2023). Anomaly Detection for Industrial Internet of Things Cyberattacks. *Computer Systems Science & Engineering*, *44*(3).

[10] Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, *59*, 102334.

[11] Görmez, Y., Arslan, H., IŞIK, Y. E., & Dadaş, İ. E. (2023). A User and Entity Behavior Analysis for SIEM Systems: Preprocessing of The Computer Emergency and Response Team Dataset. *Journal of Soft Computing and Artificial Intelligence*, *4*(1), 1-6.

[12] Basile, C., Regano, L., & Settanni, F. Towards intelligence driven automated incident response.

[13] Möller, D. P. (2023). Threats and Threat Intelligence. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 71-129). Cham: Springer Nature Switzerland.

[14] Rahaman, M. S., Islam, A., Cerny, T., & Hutton, S. (2023). Static-Analysis-Based Solutions to Security Challenges in Cloud-Native Systems: Systematic Mapping Study. *Sensors*, *23*(4), 1755.

[15] Bharadiya, J. P. (2023). A Comparative Study of Business Intelligence and Artificial Intelligence with Big Data Analytics. *American Journal of Artificial Intelligence*, *7*(1), 24.

[16] Pilling, F., Ali Akmal, H., Lindley, J., Gradinar, A., & Coulton, P. (2023). making AI-Infused products and Services more legible. *Leonardo*, *56*(2), 170-176.

[17] Negi, P., Singh, R., Gehlot, A., Kathuria, S., Thakur, A. K., Gupta, L. R., & Abbas, M. (2023). Specific Soft Computing Strategies for the Digitalization of Infrastructure and its Sustainability: A Comprehensive Analysis. *Archives of Computational Methods in Engineering*, 1-22.

[18] Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., ... &Luzcando, E. (2022). Practical Adoption of Cloud Computing in Power Systems—Drivers, Challenges, Guidance, and Real-World Use Cases. *IEEE Transactions on Smart Grid*, *13*(3), 2390-2411.

[19] Ismatullaev, U. V. U., & Kim, S. H. (2022). Review of the factors affecting acceptance of AI-infused systems. *Human Factors*, 00187208211064707.

[20] Kamikubo, R., Wang, L., Marte, C., Mahmood, A., &Kacorri, H. (2022, October). Data representativeness in accessibility datasets: A meta-analysis. In *Proceedings of the 24th International ACM SIGACCESS Conference on Computers and Accessibility* (pp. 1-15).

[21] Božić, V. Using Artifical Intelligence in Triage Process: Benefits, Challenges, and Considerations.

[22] Himeur, Y., Elnour, M., Fadli, F., Meskin, N., Petri, I., Rezgui, Y., ... & Amira, A. (2023). AI-big data analytics for building automation and management systems: a survey, actual challenges and future perspectives. *Artificial Intelligence Review*, *56*(6), 4929-5021.

[23] Aziz, L. A. R., &Andriansyah, Y. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. *Reviews of Contemporary Business Analytics*, *6*(1), 110-132.

[24] Mustafa, I. S., Nahmatwlla, L. L., & Ahmed, W. A. ROLE OF AI AND MACHINE LEARNING BASED ON PRINCIPLES OF WEB TECHNOLOGY AND CLOUD COMPUTING.

[25] Hernandez-Jaimes, M. L., Martinez-Cruz, A., Ramírez-Gutiérrez, K. A., & Feregrino-Uribe, C. (2023). Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. *Internet of Things*, 100887.

[26] Loukasmäki, H. (2023). Cyber Incident Response in Public Cloud: implications of modern cloud computing characteristics for cyber incident response.

[27] Theodoropoulos, T., Rosa, L., Benzaid, C., Gray, P., Marin, E., Makris, A., ... &Tserpes, K. (2023). Security in Cloud-Native Services: A Survey. *Journal of Cybersecurity and Privacy*, *3*(4), 758-793.

[28] Anandita Iyer, A., & Umadevi, K. S. (2023). Role of AI and Its Impact on the Development of Cyber Security Applications. In *Artificial Intelligence and Cyber Security in Industry 4.0* (pp. 23-46). Singapore: Springer Nature Singapore.

[29] Aruna, E. R., Rama Mohan Reddy, A., & Sunitha, K. V. N. (2022). Secure SDLC Using Security Patterns 2.0. In *IOT with Smart Systems: Proceedings of ICTIS 2021, Volume 2* (pp. 699-708). Springer Singapore.

[30] Islam, R., Patamsetti, V., Gadhi, A., Gondu, R. M., Bandaru, C. M., Kesani, S. C., & Abiona, O. (2023). The Future of Cloud Computing: Benefits and Challenges. *International Journal of Communications, Network and System Sciences*, *16*(4), 53-65.

[31] Mallikarjunaradhya, V., Pothukuchi, A. S., & Kota, L. V. (2023). An Overview of the Strategic Advantages of AI-Powered Threat Intelligence in the Cloud. *Journal of Science & Technology*, *4*(4), 1-12.
[32] Mungoli, N. (2023). Scalable, Distributed AI Frameworks: Leveraging Cloud Computing for Enhanced Deep Learning Performance and Efficiency. *arXiv preprint arXiv:2304.13738*.
[33] Gundu, S. R., Charanarur, P., Chandelkar, K. K., Samanta, D., Poonia, R. C., & Chakraborty, P. (2022). Sixth-generation (6G) mobile cloud security and privacy risks for AI system using high-performance computing implementation. *Wireless Communications and Mobile Computing*, *2022*, 1-14.