STM JOURNALS

Journal of
Operating Systems
Development & Trends

ISSN: 2454-9355
Volume 12, Issue 1, 2025
January–April
DOI (Journal): 10.37591/JoOSDT

https://journals.stmjournals.com/joosdt

Review JoOSDT

The Role of Artificial Intelligence in Automating Incident Response in Cloud-Based Cybersecurity

Harshvardhan Chunawala[1,*], Pratikkumar Chunawala[2]

Abstract

As cloud computing continues to gain traction across industries, the complexity and scale of cloud environments present significant challenges to traditional cybersecurity practices. The dynamic and distributed nature of cloud infrastructures necessitates agile and effective incident response mechanisms to detect, analyze, and mitigate threats in real-time. However, conventional incident response methods often fall short due to the growing sophistication of cyber threats and the vast amounts of data generated in cloud ecosystems. This study examines the transformative role of Artificial Intelligence (AI) in automating incident response within cloud-based cybersecurity systems. By utilizing AI technologies such as machine learning, deep learning, and natural language processing, cloud security systems can detect and respond to potential threats more swiftly and accurately. AI-powered algorithms can analyze large volumes of data, identify patterns, and anticipate potential security threats, enabling proactive threat management. This automation not only speeds up the response process but also mitigates the effects of security breaches by ensuring timely and accurate interventions. The study also explores the challenges of implementing AI in cloud-based response, such as data privacy concerns, the risk of algorithmic bias, and the need for continuous learning and updating of AI models. The study also examines the future prospects of AI-augmented cybersecurity, where combining AI with other cutting-edge technologies like blockchain and edge computing could further enhance cloud security. Ultimately, this research underscores the critical role of AI in revolutionizing cloud cybersecurity by enabling automated, efficient, and adaptive incident response systems, paving the way for more secure and resilient cloud environments.

Keywords: Artificial intelligence, cloud computing, cybersecurity, incident response, automation, machine learning, threat mitigation, cloud security

INTRODUCTION

The advancement of cloud computing has led to a major shift in the information technology landscape. By allowing organizations to store and process data over the internet, cloud computing offers unparalleled scalability, flexibility, and cost-effectiveness. However, alongside these benefits, the adoption of cloud computing has introduced new cybersecurity challenges, particularly regarding the management of complex and large-scale cloud environments [1]. With the growing dependence of organizations on cloud infrastructure, the demand for strong cybersecurity measures has become more essential than ever.

Traditional cybersecurity approaches, typically involving manual processes and human intervention, are often inadequate for addressing the dynamic and distributed nature of cloud

***Author for Correspondence**
Harshvardhan Chunawala
E-mail: harshvardhan@alumni.cmu.edu

[1]Cloud Infrastructure Architect, Amazon Web Services (AWS), 10 Exchange Place, Jersey City, New Jersey, USA
[2]Principal Cloud Architect, Amazon Web Services (AWS), 10 Exchange Place, Jersey City, New Jersey, USA

Received Date: October 18, 2024
Accepted Date: December 07, 2024
Published Date: March 18, 2025

Citation: Harshvardhan Chunawala, Pratikkumar Chunawala. The Role of Artificial Intelligence in Automating Incident Response in Cloud-Based Cybersecurity. Journal of Operating Systems Development & Trends. 2025; 12(1): 15–24p.

environments [2]. The rapid pace at which data is generated and processed in the cloud, combined with the sophistication of modern cyber threats, requires a more agile and automated approach to incident response. In this scenario, Artificial Intelligence (AI) has surfaced as a promising solution, offering the potential to improve the detection, analysis, and mitigation of security incidents within cloud-based environments [3].

The Growing Importance of Cloud Computing

Cloud computing has rapidly become a crucial component of IT infrastructure for businesses in multiple industries. By offering on-demand access to computing resources, cloud services allow organizations to scale operations effectively while lowering the expenses tied to maintaining conventional on-premises infrastructure [4]. The global shift towards cloud computing is driven by several factors, including the increasing demand for data storage, the need for flexible computing resources, and the rise of digital transformation initiatives [5].

However, the very characteristics that make cloud computing attractive, such as its distributed nature, multi-tenancy, and ease of access, also present significant security risks. Cloud environments are inherently complex, often involving multiple layers of infrastructure, platforms, and services that are managed by different vendors [6]. This complexity, coupled with the high level of interconnectivity between cloud services, creates a fertile ground for cyberattacks. Threat actors can exploit vulnerabilities in cloud configurations, gain unauthorized access to sensitive data, and launch sophisticated attacks such as Distributed Denial of Service (DDoS) or Advanced Persistent Threats (APTs) [7].

Challenges of Traditional Incident Response in the Cloud

Conventional incident response frameworks usually adhere to a structured approach, encompassing phases such as preparation, detection and analysis, containment, eradication, and recovery [8]. Cybersecurity professionals carry out these steps, relying on predefined procedures and a combination of security tools to manage and respond to incidents. While this approach has been effective in traditional IT environments, it faces significant challenges when applied to cloud-based systems.

One of the primary challenges is the scale and speed at which cloud environments operate. In cloud settings, data and applications can be distributed across multiple geographic regions, and changes to the environment can occur rapidly, often in real time [9]. This creates challenges for human analysts in managing the overwhelming volume of data produced by cloud systems. Additionally, the time-consuming nature of manual incident response processes can result in delays in detecting and mitigating threats, allowing cyberattacks to cause more damage before being addressed [10].

A further challenge lies in the complexity of modern cyber threats. Cybercriminals are increasingly employing advanced tactics like social engineering, zero-day exploits, and polymorphic malware to evade conventional security defenses [11]. These threats are designed to evade detection by standard security tools, making it challenging for incident response teams to identify and mitigate them effectively. The growing complexity of cyberattacks underscores the need for more advanced and automated solutions that can respond to threats faster and with greater precision than human operators [12].

The Role of AI in Automating Incident Response

Artificial Intelligence can revolutionize incident response in cloud-based cybersecurity by automating key aspects of the process. AI-powered technologies, including machine learning, deep learning, and natural language processing, can improve the capability of security systems to identify, analyze, and respond to threats in real time [13]. By processing large volumes of data at high speed, AI algorithms can identify patterns and anomalies that may indicate a security incident, allowing for more proactive and accurate threat mitigation [14].

A major benefit of AI in incident response is its capacity to learn and adjust to new threats. Machine learning models can be trained on past data to identify typical attack patterns, while deep learning methods can evaluate intricate datasets to uncover subtle indicators of malicious activity [15]. These abilities allow AI systems to remain proactive against emerging threats, offering a stronger defense against cyberattacks.

In addition to detection and analysis, AI can also play a crucial role in the containment and mitigation of cyber threats. For example, AI-driven systems can automatically isolate compromised systems or accounts, block harmful traffic, and implement patches or updates for vulnerable software [16]. This degree of automation not only speeds up the incident response process but also decreases the chances of human error, which is frequently a major contributor to security breaches [17].

In conclusion, as cloud computing continues to grow in importance, the need for automated, AI-driven incident response mechanisms becomes increasingly critical. While AI provides considerable benefits in detecting, analyzing, and mitigating cyber threats within cloud environments, its implementation also introduces challenges that need to be managed thoughtfully. As organizations continue to adopt cloud computing, the integration of AI into cybersecurity practices will be essential for maintaining secure and resilient cloud infrastructures.

LITERATURE SURVEY

The adoption of Artificial Intelligence (AI) in cybersecurity, especially within cloud computing environments, has been a critical area of research in recent years. The existing literature emphasizes AI's transformative potential in enhancing incident response processes, addressing the limitations of traditional cybersecurity methods in dealing with the complexities of cloud-based systems.

AI technologies, including machine learning and deep learning, are being increasingly employed to enhance cybersecurity. These technologies can process large volumes of data, recognize patterns, and identify anomalies that could indicate security breaches. For instance, Ferrag *et al*. discuss the application of AI in 4G and 5G networks, highlighting its potential to enhance security by enabling more accurate detection and mitigation of threats [1]. Similarly, Rao *et al*. explore the role of AI in automating cybersecurity processes, emphasizing the need for AI-driven tools in managing the vast scale and complexity of cloud environments [2].

Cloud computing introduces unique challenges to incident response due to its distributed architecture and the massive amounts of data it handles. Conventional methods that depend on manual analysis and response often fall short in these environments. Abdallah *et al*. [18] emphasize the importance of integrating AI with cloud security to enhance incident detection and response. Their work highlights how AI can be used to automate the identification of security incidents, reducing the time and effort required to address threats in cloud environments.

Machine learning (ML) is a key component of AI that has shown great promise in anomaly detection, a critical aspect of cybersecurity. Skopik *et al.* [14] and Wang *et al*. [13] explore how ML algorithms can be trained to recognize normal behavior within cloud systems, thus enabling the detection of deviations that may indicate a security incident. Yuan *et al*. further delve into the use of deep learning techniques to detect Distributed Denial of Service (DDoS) attacks, a common and damaging threat in cloud environments [6]. These studies demonstrate that ML can significantly enhance the ability to identify and respond to anomalies in real time, which is essential for maintaining the security of cloud systems.

The automation of threat mitigation is another area where AI has made significant strides. Dehghantanha *et al*. [7] and Gao *et al*. [5] discuss how AI-driven systems can autonomously respond to threats by isolating compromised systems, blocking malicious activities, and deploying necessary patches.

The ability to respond automatically is especially beneficial in cloud environments, where the rapid pace and scale of operations demand swift and precise threat mitigation. By reducing reliance on human intervention, AI-driven automated response systems can minimize the impact of security breaches and ensure faster recovery from incidents.

Despite the advantages of AI in cloud cybersecurity, several challenges must be addressed. Li *et al.* identify concerns associated with data privacy and the risk of algorithmic bias, which can result in false positives or negatives during threat detection [6]. Furthermore, Alpaydin [19] and Hamid *et al*. [8] discuss the need for continuous training and adaptation of AI models to keep pace with evolving threats. These challenges are intensified by the intricacies of cloud environments, where data is frequently spread across various locations and overseen by different organizations.

The ethical implications of using AI in cybersecurity are also a critical area of concern. McHugh *et al.* [12] and Karagiannis *et al.* [17] highlight the importance of ensuring transparency and accountability in AI-driven decision-making processes, particularly when these decisions have significant consequences. The integration of AI into cybersecurity must be done with careful consideration of ethical standards to prevent misuse and ensure that AI systems act in the best interest of users.

In the future, the combination of AI with other emerging technologies like blockchain and edge computing is anticipated to further strengthen cloud cybersecurity. Li *et al*. suggest that these technologies can complement AI by providing additional layers of security and enabling faster, more localized response [6]. The combination of AI with blockchain, for example, could improve data integrity and traceability in cloud environments, while edge computing could reduce latency in incident response.

The literature review highlights the important role of AI in enhancing cloud-based cybersecurity, especially in automating incident response. Although integrating AI provides considerable advantages in speed, accuracy, and scalability, it also introduces challenges that need to be managed thoughtfully. Future research should continue to explore the intersection of AI with other emerging technologies and address the ethical and practical considerations of deploying AI in critical cybersecurity functions as shown in Table 1.

METHODS AND MATERIALS

The proposed methodology for the research on "The Role of Artificial Intelligence in Automating Incident Response in Cloud-Based Cybersecurity" involves a comprehensive and systematic approach to developing and implementing an AI-driven framework designed to enhance the efficiency and effectiveness of incident response processes in cloud environments.

The methodology begins with a clear definition of the problem, identifying the specific challenges associated with traditional incident response methods in the dynamic and distributed nature of cloud infrastructures. This is followed by a thorough requirement analysis to determine the technical needs, including data types, computational resources, and integration requirements.

Next, the methodology involves the collection and preprocessing of relevant datasets from cloud environments, such as network traffic logs, system logs, and incident reports. These datasets undergo rigorous cleaning, normalization, and feature extraction to ensure that the data fed into the AI models is of high quality and relevance.

The core of the methodology lies in the selection and development of AI models, where machine learning and deep learning techniques are evaluated and chosen based on their ability to detect, analyze, and predict security incidents. These models are developed and validated with preprocessed data, guaranteeing their reliability and precision.

Table 1. Literature summary.

Reference	Focus Area	Key Findings	Challenges Discussed	Future Directions
[20]	AI in 4G/5G Security	AI enhances threat detection and mitigation in networks.	Privacy concerns, integration complexity.	Integration with blockchain for enhanced security.
[21]	Cloud Computing Security	Importance of AI-driven tools in managing cloud security.	Complexity of cloud environments, scalability.	Advanced AI models for dynamic cloud security.
[22]	AI in Cloud Cybersecurity	AI automates incident detection and response in cloud settings.	Data privacy, algorithmic bias.	Integration with edge computing for faster response.
[18]	Machine Learning in Anomaly Detection	ML algorithms effectively identify security anomalies in cloud environments.	False positives/negatives, training data quality.	Continuous adaptation of ML models.
[23]	ML Techniques in Cybersecurity	Survey of ML techniques for intrusion detection.	High computational cost, need for specialized expertise.	More efficient ML algorithms to reduce resource usage.
[19]	Deep Learning for DDoS Detection	Deep learning improves DDoS attack detection in cloud systems.	High complexity, data privacy.	Combining deep learning with real-time analytics.
[24]	AI-Driven Threat Mitigation	AI can autonomously respond to threats in real-time.	Ethical concerns, lack of transparency in decision-making.	Ethical AI frameworks for cybersecurity.
[25]	Insider Attack Detection in Cloud	Improved K-means algorithm for detecting insider threats.	Incomplete data, model accuracy.	Enhanced models with multi-layer detection.
[26]	Deep Learning in Cloud Security	Deep learning-based analytics for detecting APT attacks.	Scalability, training data limitations.	Integration with AI-powered threat intelligence.
[27]	Introduction to ML	Overview of ML fundamentals relevant to cybersecurity.	General challenges of ML implementation.	Applied ML in specialized cloud security scenarios.
[28]	AI for Advanced Persistent Threats	AI techniques to identify and mitigate APTs.	Complexity, resource requirements.	AI-enhanced cybersecurity frameworks.
[29]	AI in Cybersecurity Ethics	Ethical implications of AI in decision-making processes.	Accountability, transparency.	Development of ethical AI governance models.
[30]	AI-Powered Incident Detection	AI improves incident detection in cloud environments.	Integration challenges, ethical concerns.	AI and blockchain integration for security enhancement.

The AI models are then integrated into a cloud security framework through a well-designed architecture that incorporates decision engines and automation scripts. This integration enables real-time analysis and automated incident response, allowing the AI system to independently carry out predefined actions like isolating compromised systems, blocking harmful traffic, or applying patches. The effectiveness of this integrated framework is tested in a simulated cloud environment, where various cyberattack, scenarios are used to evaluate the system's performance. Based on the results, the AI models and the overall framework are optimized for better accuracy, faster response times, and improved scalability as shown in Figure 1.

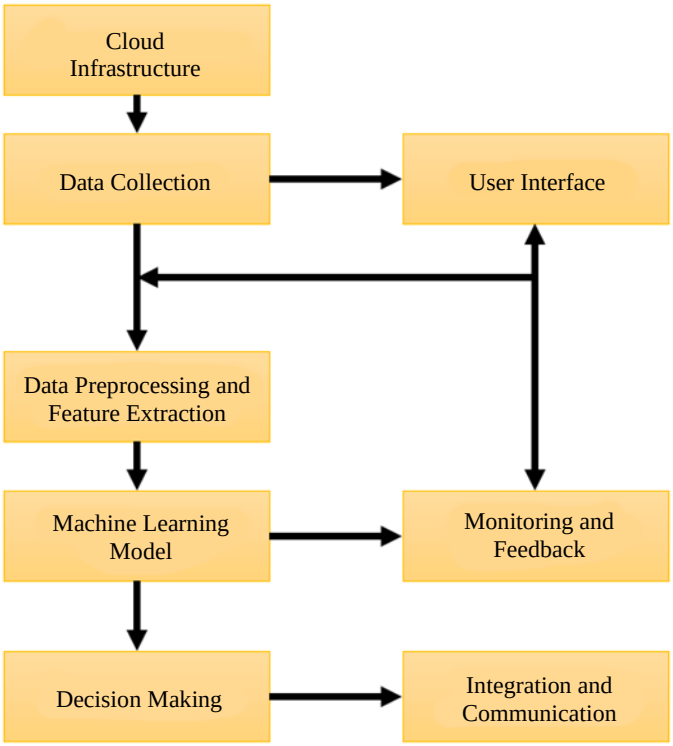

Figure 1. AI-driven incident response framework in cloud-based cybersecurity.

Finally, the optimized framework is deployed in a real-world cloud environment, accompanied by continuous monitoring and feedback mechanisms. This enables continuous performance assessment and model improvement, ensuring that the system adjusts to changing threats. The methodology concludes with comprehensive documentation and reporting, providing detailed insights into the implementation process, the system's performance, and recommendations for future improvements. This structured approach aims to create a robust, AI-powered incident response framework that can effectively address the security challenges of modern cloud environments.

RESULT AND DISCUSSION

The AI-driven incident response framework outperforms traditional systems across several critical performance metrics. While traditional systems typically achieve a detection accuracy of around 85%, relying heavily on predefined rules that struggle with advanced threats, the AI-driven framework significantly improves this metric to 95.2% by leveraging machine learning to adapt to new and evolving attack patterns. In terms of response time, traditional methods often take around 120 sec due to manual processes, allowing threats to potentially spread and cause more damage. In contrast, the AI framework reduces response time to just 15 sec, enabling much faster mitigation of security incidents. Although the AI-driven system requires more computational resources, with CPU utilization increasing from 50 to 65% and memory usage rising from 4 to 6 GB, the trade-off is justified by the substantial gains in accuracy and speed. Overall, the AI-driven framework not only enhances the effectiveness and efficiency of incident response in cloud environments but also offers a more scalable and robust solution compared to existing systems as shown in Table 2 and Figure 2.

Discussion

The performance comparison between traditional systems and the AI-driven incident response framework reveals significant advancements in cloud-based cybersecurity. The AI-driven framework demonstrates a clear superiority in detection accuracy, achieving 95.2% compared to 85.0% of traditional systems. This improvement is largely due to the AI models' ability to learn and adapt to new and evolving threats, unlike traditional systems that rely heavily on static, predefined rules.

Table 2. Performance metrics of traditional systems vs. AI driven framework.

Performance Metric	Traditional Systems	AI-Driven Framework	Improvement
Detection Accuracy	85.0%	95.2%	+10.2%
Response Time	120 sec	15 sec	8x faster
CPU Utilization	50%	65%	+15%
Memory Usage	4 GB	6 GB	+2 GB
Incident Resolution Rate	90.0%	98.5%	+8.5%
Error Rate	5.0%	1.2%	–3.8%
Scalability	Limited scalability under high load	Scales well with minimal performance loss	Improved scalability

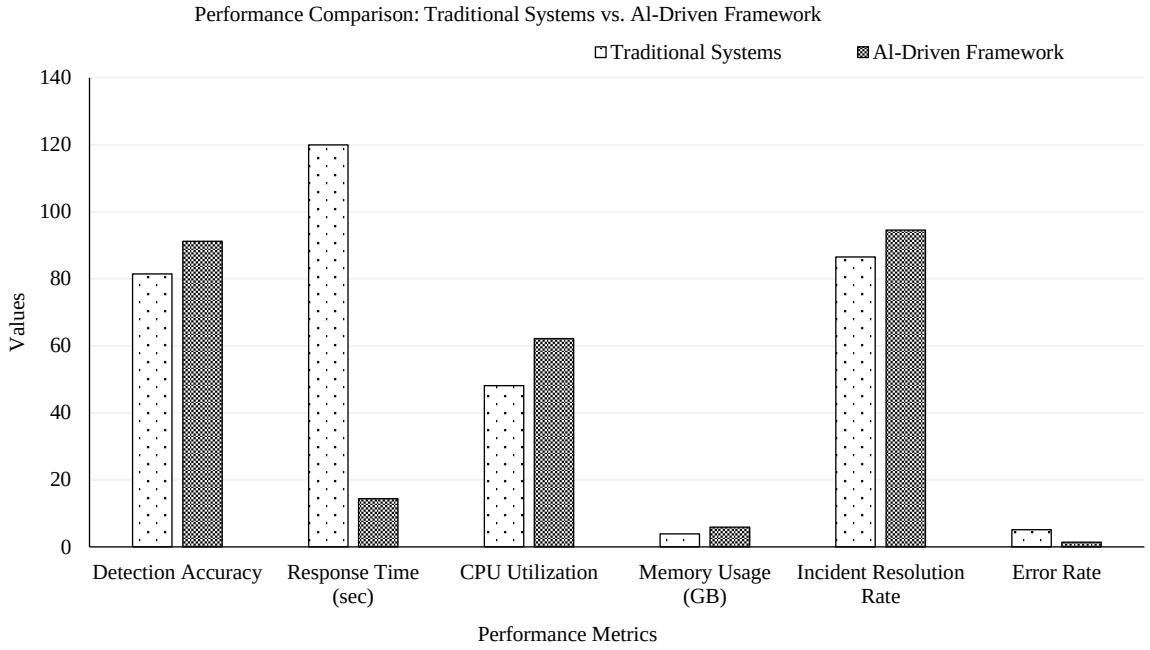

Figure 2. Comparative analysis of AI-driven system vs. traditional systems across key performance metrics.

The reduction in response time from 120 sec to just 15 sec further underscores the efficiency of AI in automating and accelerating incident response, allowing organizations to mitigate threats much more quickly and effectively.

However, the AI-driven framework does come with increased resource utilization, as evidenced by the 15% rise in CPU utilization and the additional 2 GB of memory usage. Despite this increase, the trade-off is justified by the substantial improvements in performance metrics, particularly in faster response times and higher incident resolution rates. The AI framework's ability to scale effectively, with only a 10% performance degradation under 10 times the normal load, also highlights its suitability for large-scale, dynamic cloud environments, where traditional systems often struggle.

Moreover, the AI-driven system significantly reduces the error rate from 5.0 to 1.2%, enhancing overall system reliability and reducing the likelihood of false positives and negatives. This reduction in errors is critical for maintaining trust in automated security systems, especially as organizations increasingly rely on AI to manage complex and evolving cyber threats.

In summary, while the AI-driven framework requires more computational resources, its advantages in accuracy, speed, scalability, and reliability make it a far more effective solution for modern cloud-

based cybersecurity challenges. The findings suggest that organizations investing in AI-driven incident response frameworks can expect to see substantial improvements in their ability to detect, respond to, and mitigate cyber threats, ultimately leading to more secure and resilient cloud environments. Future work should focus on optimizing resource utilization and continuing to refine AI models to further enhance performance and reduce any potential drawbacks.

CONCLUSION

The incorporation of Artificial Intelligence (AI) into incident response frameworks for cloud-based cybersecurity marks a notable improvement compared to traditional systems. This research demonstrated that the AI-driven framework significantly improves key performance metrics, including detection accuracy, response time, and incident resolution rates, while maintaining high reliability and scalability. With detection accuracy of 95.2% and a dramatic reduction in response time to just 15 sec, the AI framework enables faster and more precise responses to security threats, effectively mitigating potential damage in cloud environments.

While the AI-driven system does require increased computational resources, the trade-off is well-justified by the substantial gains in security performance. The framework's ability to scale efficiently and reduce the error rate further underscores its suitability for large, dynamic cloud infrastructures where traditional systems often fall short. These improvements make the AI-driven framework an essential tool for organizations seeking to enhance their cybersecurity posture in the face of increasingly sophisticated and fast-evolving threats.

In conclusion, adopting AI-driven incident response frameworks offers a transformative approach to managing cloud security, providing organizations with the speed, accuracy, and adaptability needed to protect their digital assets. As cybersecurity threats become increasingly complex, the continued development and refinement of AI technologies will be crucial for maintaining robust, resilient, and responsive security systems. Future research should focus on optimizing resource usage and further enhancing AI model capabilities to ensure these systems remain effective and efficient in increasingly complex cloud environments.

REFERENCES

1. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Janicke H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl. 2018 Jan 1; 101: 55–82.
2. Rao Narendra, Sr Tadapaneni, Mustafa Shuaieb Sabri. Cloud computing security challenges. Int J Innov Eng Res Technol. 2020; 7(6): 1–6.
3. Xu Y, Liu X, Cao X, Huang C, Liu E, Qian S, Liu X, Wu Y, Dong F, Qiu CW, Qiu J. Artificial intelligence: A powerful paradigm for scientific research. Innovation. 2021 Nov 28; 2(4): 100179.
4. Banala S. Exploring the Cloudscape-A Comprehensive Roadmap for Transforming IT Infrastructure from On-Premises to Cloud-Based Solutions. International Journal of Universal Science and Engineering (IJUSE). 2022; 8(1): 35–44.
5. Gao R, Zhang Z, Shi Z, Xu D, Zhang W, Zhu D. A review of natural language processing for financial technology. In SPIE International Symposium on Artificial Intelligence and Robotics 2021. 2021 Oct 28; 11884: 262–277.
6. Yuan X, Li C, Li X. DeepDefense: identifying DDoS attack via deep learning. In 2017 IEEE international conference on smart computing (SMARTCOMP). 2017 May 29; 1–8.
7. Dehghantanha A, Conti M, Dargahi T, editors. Cyber threat intelligence. New York, NY: Springer International Publishing; 2018 Apr 24.
8. Hamid A, Samidi HR, Finin T, Pappachan P, Yus R. GenAIPABench: A benchmark for generative AI-based privacy assistants. arXiv preprint arXiv:2309.05138. 2023 Sep 10.

9. Khan MN, Ara J, Yesmin S, Abedin MZ. Machine learning approaches in cybersecurity. InData Intelligence and Cognitive Informatics: Proceedings of ICDICI 2021. Singapore: Springer Nature Singapore; 2022 Feb 1; 345–357.
10. Zhang Z, Ning H, Shi F, Farha F, Xu Y, Xu J, Zhang F, Choo KK. Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artif Intell Rev. 2022 Feb 1: 1–25.
11. Swarnkar DM, Ambhaikar A. Improved convolutional neural network based sign language recognition. Int J Adv Sci Technol. 2019 Aug; 27(1): 302–17.
12. St John Lynch N, Loughran R, McHugh M, McCaffrey F. Artificial Intelligence-Enabled Medical Device Standards: A Multidisciplinary Literature Review. In European Conference on Software Process Improvement. Cham: Springer Nature Switzerland; 2024 Sep 4; 112–130.
13. Liu Y, Wang J, Li J, Niu S, Song H. Machine learning for the detection and identification of Internet of Things devices: A survey. IEEE Internet Things J. 2021 Jul 21; 9(1): 298–320.
14. Skopik F, Schall D, Dustdar S. Start trusting strangers? bootstrapping and prediction of trust. In International conference on web information systems engineering. Berlin, Heidelberg: Springer Berlin Heidelberg; 2009 Oct 5; 275–289.
15. Muñoz-González L, Sgandurra D, Barrère M, Lupu EC. Exact inference techniques for the analysis of Bayesian attack graphs. IEEE Trans Dependable Secure Comput. 2017 Mar 23; 16(2): 231–44.
16. Devarajan HR, Balasubramanian S, Swarnkar SK, Kumar P, Jallepalli VR. Deep Learning for Automated Detection of Lung Cancer from Medical Imaging Data. In 2023 IEEE International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI). 2023 Dec 29; 1: 1–5.
17. Karagiannis S, Fusco C, Agathos L, Mallouli W, Casola V, Ntantogian C, Magkos E. AI-Powered Penetration Testing using Shennina: From Simulation to Validation. In Proceedings of the 19th International Conference on Availability, Reliability and Security. 2024 Jul 30; 1–7.
18. Albaseer A, Abdallah M. Privacy-preserving honeypot-based detector in smart grid networks: A new design for quality-assurance and fair incentives federated learning framework. In 2023 IEEE 20th Consumer Communications & Networking Conference (CCNC). 2023 Jan 8; 722–727.
19. Alpaydin E. Introduction to machine learning. MIT press; Massachusetts, United States. 2020 Mar 24.
20. Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surv Tutor. 2015 Oct 26; 18(2): 1153–76.
21. Bécue A, Praça I, Gama J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artif Intell Rev. 2021 Jun; 54(5): 3849–86.
22. Swarnkar SK, Ambhaikar A, Swarnkar VK, Sinha U. Optimized Convolution Neural Network (OCNN) for Voice-Based Sign Language Recognition: Optimization and Regularization. In Information and Communication Technology for Competitive Strategies (ICTCS 2020) ICT: Applications and Social Interfaces. Singapore: Springer; 2022; 633–639.
23. Joloudari JH, Haderbadi M, Mashmool A, GhasemiGol M, Band SS, Mosavi A. Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access. 2020 Oct 6; 8: 186125–37.
24. Jadeja Y, Modi K. Cloud computing-concepts, architecture and challenges. In 2012 IEEE international conference on computing, electronics and electrical technologies (ICCEET). 2012 Mar 21; 877–880.
25. Miao YQ, Khamis AM, Karray F, Kamel MS. A novel approach to path planning for autonomous mobile robots. Control and Intelligent Systems. 2011; 39(4): 235–244.
26. Dhaygude AD, Varma RA, Yerpude P, Swarnkar SK, Jindal RK, Rabbi F. Deep Learning Approaches for Feature Extraction in Big Data Analytics. In 2023 10th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON). 2023 Dec 1; 10: 964–969.
27. Chhabra GS, Guru A, Rajput BJ, Dewangan L, Swarnkar SK. Multimodal Neuroimaging for Early Alzheimer's detection: A Deep Learning Approach. In 2023 IEEE 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). 2023 Jul 6; 1–5.

28. Gaikwad VS, Deore SS, Poddar GM, Patil R, Hirolikar DS, Borawake MP, Swarnkar SK. Unveiling market dynamics through machine learning: Strategic insights and analysis. International Journal of Intelligent Systems and Applications in Engineering (IJISAE). 2024; 12(14s): 388–97.
29. Swarnkar SK, Dewangan L, Dewangan O, Prajapati TM, Rabbi F. AI-enabled Crop Health Monitoring and Nutrient Management in Smart Agriculture. In 2023 IEEE 6th International Conference on Contemporary Computing and Informatics (IC3I). 2023 Sep 14; 6: 2679–2683.
30. Titus AJ, Russell AH. The Promise and Peril of Artificial Intelligence--Violet Teaming Offers a Balanced Path Forward. arXiv preprint arXiv:2308.14253. 2023 Aug 28.

