Computer Fraud and Security
ISSN (online): 1873-7056

Artificial Intelligence Techniques for Real-Time Cyber Threat Detection in Cloud Computing Environments

Nithish Yadav Thotla
Independent Researcher
Missouri University of Science and Technology, USA
nithishthotla@gmail.com

Abstract

Artificial intelligence has become a vital technology that has been used to enhance cloud cybersecurity through real-time detection of cyber threats and automatic incident response. Traditional rule-based security mechanisms usually have challenges with detecting zero-day attacks, behavioural anomalies, and evolving threats in cloud-native infrastructure. This paper focuses on the use of Artificial Intelligence (AI) methods such as Machine Learning (ML), Deep Learning (DL), and hybrid AI in enhancing cyber threat detection, response time, and cloud security performance. The paper uses a secondary data collection strategy involving peer-reviewed journal articles, cybersecurity reports and industry literature. A qualitative research design has been adopted to analyse the existing evidence in an inductive approach. Thematic analysis has been used to analyse different themes in the literature, such as AI technologies for threat detection, detection accuracy, response time, real-time monitoring, and cloud security performance. The results show that AI-based Intrusion Detection Systems detect different cyber threats such as DDoS attacks, IoT attacks, phishing attacks and industrial denial-of-service attacks with a detection accuracy of 94%-99.99%. Moreover, the use of AI-based technology results in a significant reduction in the MTTD and MTTR of 30-50% by providing continuous monitoring and automated reaction capabilities to enhance organisational resilience. In addition, the study notes that risk management, network perimeter security, and business continuity are still among the main cybersecurity concerns in cloud computing. The study concludes that using AI for cyber threat detection is scalable, precise, and proactive. Using AI with continuous monitoring, Zero Trust strategy, and DevSecOps can enhance cloud security from cyber threats.

Keywords: Artificial intelligence, cloud computing, cyber threat detection, machine learning, deep learning, cloud security, intrusion detection, real-time monitoring.

Introduction

Cloud-native technologies enhance the scalability, flexibility, and efficiency of applications by utilising containers, microservices, Kubernetes, and serverless technology. Nevertheless, the distributed nature of these technologies raises cybersecurity challenges in terms of applications, networks, and infrastructure security. In 2023, about 90% of organisations applied cloud-native technologies to develop and deploy applications; therefore, the need to secure containerised environments became crucial. Kubernetes remained the dominant container orchestration technology, with the share of about 66% of organizations that used Kubernetes in production in 2023. Containerised applications are subject to vulnerabilities from insecure container images, privilege escalation, container escape, and unauthorised access to shared resources. According to the 2023 CNCF Annual Survey, 67% of firms have faced security problems involving Kubernetes configuration and management. Microservices create even more issues regarding security since many services interact via APIs and service meshes. Additionally, Cloudflare mentioned that it mitigated 14 million DDoS attacks in 2023, which shows how the scale of such attacks on the cloud environment is growing. Cloud-native systems produce enormous amounts of telemetry and network logs; thus, monitoring should be automated. This means that intrusion detection, continuous monitoring, safe container management, DevSecOps principles, and proper identity management are vital for cloud-native environments.

Methods

The methodology chosen by this study in order to investigate the influence of AI-based approaches on cyber threat detection in cloud native settings was the secondary data collection approach. The use of secondary data was due to the fact that such data is credible and well-published in academic journal articles, industry reports, surveys about

cybersecurity, and whitepapers. The secondary data approach provided an opportunity for the analysis of the current state of affairs in the field using existing knowledge without the need to collect primary data, along with recent statistics in the field of cybersecurity (Prayitno, 2026). This framework enabled the interpretation of concepts, security threats, and AI technology usage in various cloud computing environments. The research adopted an inductive methodology, as its conclusion emerged from the analysis of already-existing evidence, not from the verification of any predefined hypothesis. Information from several studies and cybersecurity reports was analysed in order to reveal common themes related to AI-based threat detection and response, real-time monitoring, and performance of cloud security. A thematic analysis technique was used in order to structure and analyse the information gathered. The literature was analysed, coded, and categorised into several themes, such as AI technology, threat detection accuracy, reaction time, real-time monitoring, and cloud security performance. This technique was selected due to its clear structure.

Results

Performance of AI Models in Real-Time Cyber Threat Detection

Cloud-native architecture enhances scalability, flexibility, and operational efficiency using containers, microservices, and Kubernetes. The adoption rate of cloud infrastructure has grown tremendously, leading to increased security threats (Golightly *et al.* 2022). According to Forrester, the global market for public cloud will rise to $236 billion in 2020 compared to previous predictions of $191 billion in 2014 and $159 billion in 2011.

Indicator	2011	2014	2018	2020	Value
Public Cloud	$159B	$191B	—	$236B	+48%
Containers	—	—	19%	33%	+14%
NGFW Mature	—	—	—	81%	High
NGFW Immature	—	—	—	51%	Low
Monitoring Mature	—	—	—	53%	16%

Table 1: Cloud-Native Security Adoption and Infrastructure Trends

Containerization has been increasing due to the rising popularity of cloud architecture. Containers have become more popular than before and made up about 33% of hybrid cloud workloads in 2020, compared to 19% in 2018. Although containerization provides flexibility, it also creates potential security risks like insecure images, container escape, and unauthorised access. The issues related to security are aggravated due to the complexity of Kubernetes environments. As revealed in the CS²AI–KPMG 2020 Cyber Security Report, organisations that had well-developed security programs enjoyed better protection (Ogborigbo *et al.* 2024). In particular, 81% used next-generation firewalls, while only 51% did so in the case of immature security programs. Moreover, 53% continuously monitored all control system networks; meanwhile, only 16% of immature organisations managed to provide the same monitoring coverage.

Detection Accuracy Across Different Cyber Threat Types

DDoS Attack Detection: AI models have a 94% to 97% detection accuracy rate in detecting DDoS attacks in cloud-native networks. The Random Forest detects attack traffic quickly, whereas the LSTM detects sequential traffic anomalies. This is because these models analyse the packet flows, volume of traffic, and behaviour patterns in real-time (Akibis *et al.* 2024). This high detection accuracy rate helps minimise the attack duration and increase network availability.

Email and Malicious URL Detection: AI models prove to be efficient at detecting malicious emails and URLs even before reaching the user's inbox. The Support Vector Machine and Naïve Bayes algorithms attain an accuracy rate of 96.68%-99.62% for detecting spam emails. The machine learning classifiers have an accuracy of 100% in identifying the malicious URLs in benchmark datasets (Aljabri *et al*. 2022). The models perform analysis of the email contents, sender's behaviour, URLs, and domains.

IoT and Cloud Intrusion Detection: The deep learning techniques increase the intrusion detection rate for IoT systems and cloud computing at the rate of 95.25% to 99.70%. These techniques work on cloud telemetry, network traffic, and device behaviour analysis.

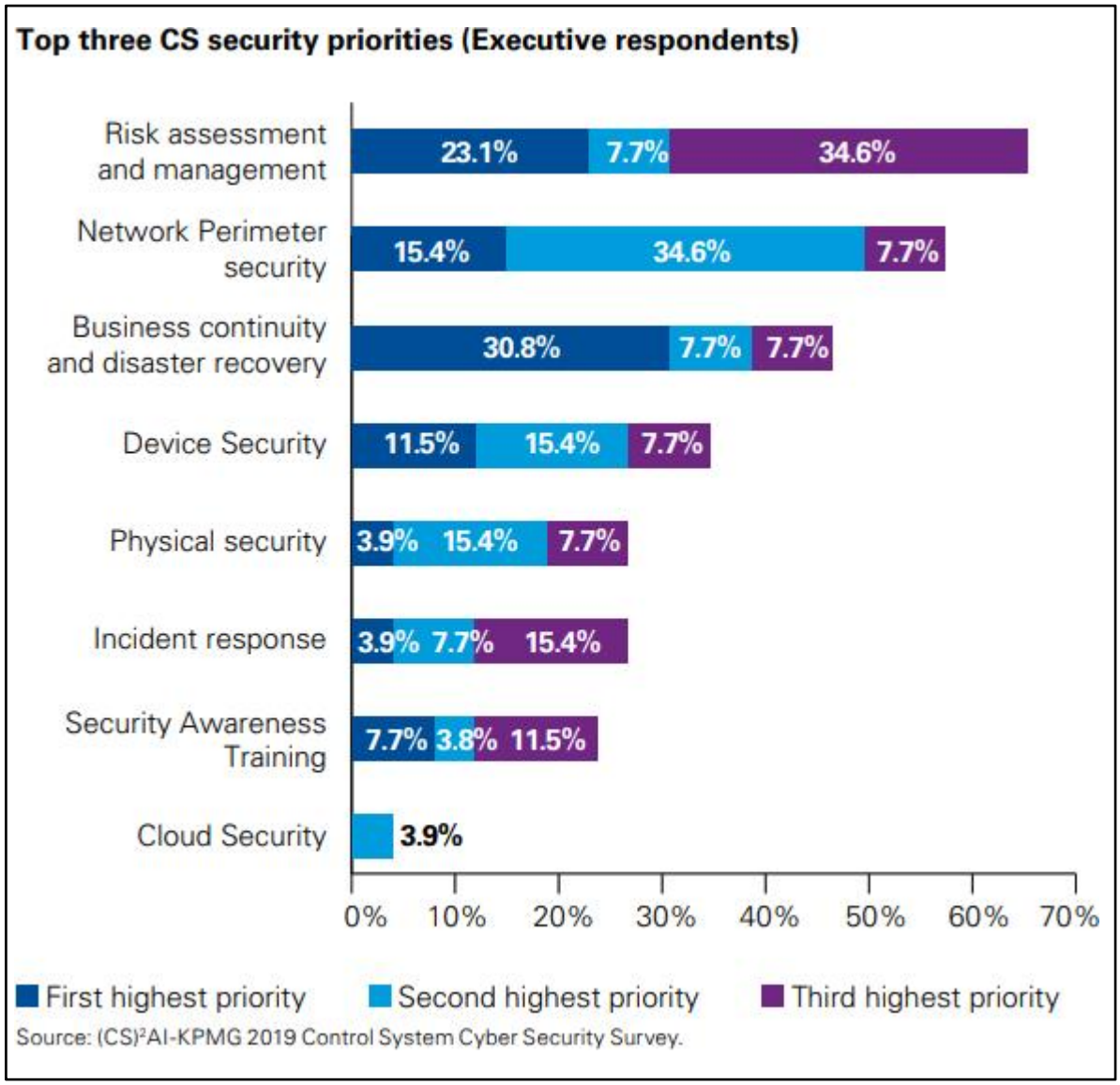

Figure 1: CS Security Key Performance Indicators (KPIs)

(Source: The CS²AI–KPMG 2020 Cyber Security Annual Report, 2020)

The CS²AI–KPMG (2020) report states that 64.5% of respondents were concerned about lowering disruption to operations, 52.7% of respondents were interested in lowering security incidents, and 47.3% wanted to lower incident response time. This highlights the necessity of accurate cyber threat detection through AI (Sivakumar *et al*. 2025). AI can detect unauthorised access, lateral movement, and even zero-day attacks without being based on known signatures.

Industrial IoT Threat Detection Performance: Accuracy is vital in industrial IoT-based detection since cyber threats may interfere with the functioning of the infrastructure (Georg, Baskar & Srikaanth, 2024). The Multi-Layer Perceptron (MLP) offers an accuracy of 99.99%, whereas the CART algorithm offers 99.98% for the detection of the denial-of-service attack in industrial networks. The hybrid AI system utilises both machine learning and deep learning to avoid false-positive detections.

Response Time and Real-Time Detection Efficiency: The metrics response time and real-time detection efficiency help determine the rate at which a system of cybersecurity identifies, analyses, and takes action against the activities carried out by attackers. The use of artificial intelligence enhances the efficiency of the detection process as it monitors cloud telemetry, network traffic, user behaviour, and application logs in real time with little delay. AI-based intrusion detection systems can cut down MTTD and **MTTR** by 30% to 50% (Mukabbir, 2025).

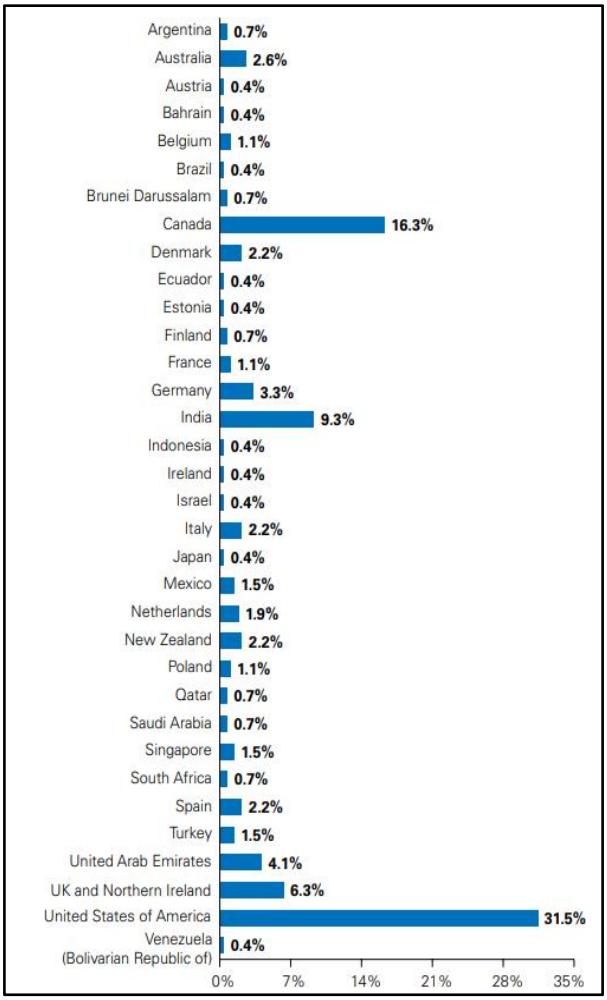

Figure 2: Geographic Distribution of Survey Respondents by Country and Region

(Source: Control System Cyber Security Association International & KPMG International, 2020)

Based on the CS²AI–KPMG 2020 Cyber Security Annual Report, 64.5% of respondents noted the reduction of operational disruptions as the most significant cyber security performance measure, showing the significance of swift detection of threats. The survey also revealed that 52.7% viewed the reduction of security incidents as a priority, whereas 47.3% of respondents emphasised the reduction of incident resolution times with the help of continuous monitoring and automation (Singh, Anand & Prabhat, 2022). The survey undertaken by CS²AI–KPMG 2020 covered many countries. The U.S. topped the list (31.5%), then India (16.3%), the UAE (9.3%), and the UK (6.3%). Such regional perspectives offer various insights on how control systems cybersecurity measures are practised as well as on how to detect real-time threats (Control System Cyber Security Association International & KPMG International, 2020). Real-time monitoring powered by artificial intelligence analyses streaming security data and triggers alerts in case any unusual behaviour or suspicious network traffic is detected. It helps to minimise downtime, increase incident visibility, and improve the resilience of distributed cloud infrastructure.

Impact of AI Techniques on Cloud Security Performance

Artificial Intelligence increases cloud security performance through better threat detection, response to incidents, anomaly detection, and network protection in cloud-native architecture. Using AI-based methods, it is possible to analyse cloud telemetry data, user activity, application logs, and network traffic in real-time to detect cyber threats more quickly and effectively. AI-based security solutions also decrease MTTD and MTTR by 30% to 50%. More than 80% of the respondents were responsible for making decisions regarding OT security expenditure (Emmanuel, 2026). The Financial Decision was made by Security Directors (32%), whereas Security Spending Approval was made by CISOs (25%). The

level of respondents included Operations (45.7%), Management (19.8%), Senior Management (15.6%), and Executive (18.9%) (Control System Cyber Security Association International & KPMG International, 2020). As per the CS²AI–KPMG 2020 Cyber Security Annual Report, 26.9% of respondents considered Risk Assessment and Management as the top cybersecurity priority, whereas 24.7% chose Network Perimeter Security as their second top priority. In addition to this, 20.4% considered Business Continuity and Disaster Recovery as the second top security priority.

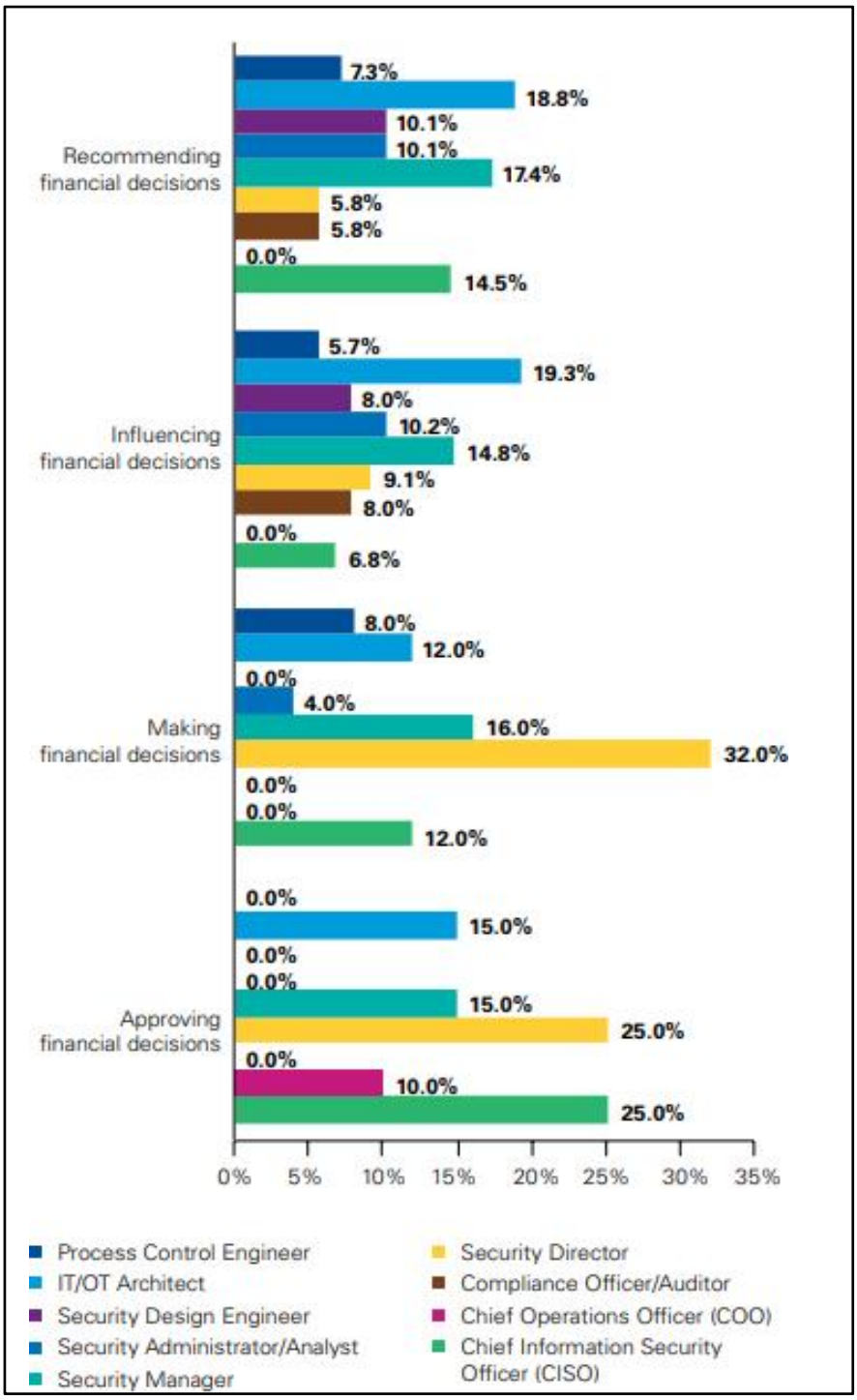

Figure 3: AI Techniques on Cloud Security Performance

(Source: Control System Cyber Security Association International & KPMG International, 2020)

The use of AI-based anomaly detection allows constant monitoring of network behaviour and identification of zero-day attacks, insider threats, and abnormal access attempts without the need for signatures alone. Automated AI-based

response systems help isolate the affected workload, block the IP address involved, and cancel suspicious credentials in real-time (Chagovec *et al.* 2026). Such aspects ensure better security resilience, minimise false positives, and facilitate proactive cybersecurity. Thus, AI methods help improve cloud security performance through intelligent monitoring, quick response time, enhanced perimeter defence, and continuous risk assessment in cloud-native environments (Control System Cyber Security Association International & KPMG International, 2020).

Comparative Evaluation of Artificial Intelligence Techniques in Cloud Environments

The different methods of artificial intelligence provide various efficiencies in cloud cybersecurity through the speed of detection, efficiency, scalability, and resource consumption.

Method	Accuracy	Speed	Scalability	Resources	Application
Random Forest	94–95%	High	High	Low	DDoS
LSTM	96–97%	High	Medium	Medium	Anomaly
SVM	92%	Medium	Low	Medium	Phishing
CNN	95%	High	Medium	High	Malware
XGBoost	96%	High	High	Low	Intrusion

Table 2: Comparative Performance of AI Methods in Cloud Cybersecurity

The Random Forest method gives a 94%–95% accuracy rate, coupled with efficient processing and minimal computational costs; thus, it is ideal for real-time DDoS attacks. LSTM models give a 96%–97% efficiency rate due to their detection of sequential patterns and behavioural anomalies in the cloud environment (Jiang, Jia & Zhang 2025). The SVM model has an efficiency rate of around 92% for phishing and spam attack detection; however, its efficiency rate is relatively low for big data cloud environments.

Discussion

The study reveals that there is a considerable increase in the detection of cybersecurity threats and improved cybersecurity performance in cloud environments by using artificial intelligence. AI helps achieve faster, more accurate, and continuous monitoring of cybersecurity threats than any other traditional signature-based cybersecurity mechanism (Khan, Arif & Khan, 2024). Machine learning algorithms like Random Forest and Support Vector Machine can detect existing cybersecurity threats easily, while deep learning algorithms like the Long Short-Term Memory model help in detecting complicated behavioural anomalies and zero-day attacks by analysing the sequence of traffic data. In addition to that, the findings show that real-time monitoring plays a vital role in mitigating cyber threats. AI intrusion detection systems cut down the mean time to detect (MTTD) and mean time to respond (MTTR) to cybersecurity threats by 30-50%. The application of hybrid AI models enhances the detection process through the combination of fast classification with behaviour-based analysis in order to decrease false positives and sustain high-level detection effectiveness (Hampiholi, 2023). The results support the CS²AI–KPMG Control System Cyber Security Annual Report (2020) findings, which have revealed that Risk Assessment and Management (26.9%), Network Perimeter Security (24.7%), and Business Continuity and Disaster Recovery (20.4%) were the top cybersecurity concerns among organisations. Also, according to the report, 64.5% of organisations have concentrated on preventing operational interruptions, and 52.7% have emphasised the reduction of security incidents through appropriate security measures. However, the use of AI technology for cloud security is still confronted with problems such as adversarial attacks, transparency, computational costs, and false positive alerts. Therefore, organisations need to integrate AI-driven detection with the principles of Zero Trust, risk assessment, and DevSecOps.

Conclusion

AI has emerged as a core technology in advancing cyber threat detection in cloud-native platforms. AI helps improve detection capabilities, enables real-time monitoring and automated response to incidents within distributed cloud infrastructure. Machine learning, deep learning, and hybrid AI models are capable of detecting various threats, including DDoS attacks, phishing, malware and cloud intrusions. It is evident from the study that continuous monitoring, risk assessment, and perimeter network security continue to be core aspects of cloud security. Challenges such as adversarial

attacks, false positives, and computational overhead are faced by AI-driven security solutions, but it is evident that AI provides better resiliency and proactive security capabilities.

Reference List

1. Akibis, M., Pereira, J., Clark, D., Mitchell, V., & Alvarez, H. (2024). Measuring ransomware propagation patterns via network traffic analysis: An automated approach.
2. Aljabri, M., Altamimi, H. S., Albelali, S. A., Al-Harbi, M., Alhuraib, H. T., Alotaibi, N. K., ... & Salah, K. (2022). Detecting malicious URLs using machine learning techniques: review and research directions. *IEEE Access*, *10*, 121395-121417.
3. Control System Cyber Security Association International & KPMG International, (2020). *CS²AI–KPMG Control System Cyber Security Annual Report 2020*. Available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2020/10/kpmg-control-system-cyber-security-annual-report.pdf
4. George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.
5. Golightly, L., Chang, V., Xu, Q. A., Gao, X., & Liu, B. S. (2022). Adoption of cloud computing as innovation in the organization. *International journal of engineering business management*, *14*, 18479790221093992.
6. Hampiholi, N. (2023). Medical imaging enhancement with AI models for automatic disease detection and classification based on medical images. *Int. J. Eng. Appl. Sci. Technol*, *8*(5), 31-37.
7. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The most recent advances and uses of AI in cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 566-578.
8. Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., Egerson, J., ... & Owoade, Y. (2024). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. *World Journal of Advanced Research and Reviews*, *23*(1), 081-096.
9. Singh, B., Anand, A., & Prabhat, S. (2022). Real-time network monitoring and incident response with AI-driven automation data center and WAN transformation. *Available at SSRN 5331665*.