Frontiers in Computer Science and Artificial Intelligence
ISSN: 2978-8048
DOI: 10.32996/fcsai
Journal Homepage: www.al-kindipublisher.com/index.php/fcsai

FCSAI
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Hybrid Cybersecurity: AI Models for Predicting Threats Across Multi-Cloud for U.S. Business Environment

Md Mahbubul Alam [1], Md Imran Khan[2] and S M Sayem[3]

[1] College of Business Administration, Master of Science in Information Systems, Central Michigan University: Mount Pleasant, Michigan, US

ORCID ID: *https://orcid.org/0009-0008-8549-7496*

[2] College of Graduate and Professional Studies, Master of Science in Information Studies, Trine University, Angola, Indiana, USA-

ORCID ID: *https://orcid.org/0009-0004-9270-8782*

[3] College of Computer Science, Associate in applied science, Wayne county community college district, USA

ORCID ID: *https://orcid.org/0009-0007-7372-7154*

Corresponding Author: Md Imran Khan**, Email:** imran.mis.lu@gmail.com

| ABSTRACT

The presence of multipurpose cloud solutions has presented emerging cybersecurity concerns and an incentive to use more sophisticated methods, including threat prediction and mitigation. The above writing presents the integration of artificial intelligence (AI) hybrid models in multipurpose cloud infrastructures to achieve better threat prediction and detection. The hybrid AI models, achieved by implementing supervised and unsupervised learning algorithms in parallel with the fusion of data across multiple cloud platforms help to achieve new heights of accuracy, scalability, and flexibility of the cybersecurity systems. The study mentions use of deep learning, extensive data management and reinforcement learning as a real-time detection mechanism not just to detect known threats but also detect new threats. The findings indicate that hybrid AI solutions could be relevant in achieving substantial performance in terms of the threat detection rate, low false alarms, and quicker response rates in running multipurpose cloud setups. These findings confirm again the strength of hybrid AI models to cope with the dynamic nature of cybersecurity threats and, hence, enhance the system resilience and offer more efficient protection in various cloud environments. The article analyzes the embodiment of artificial intelligence (AI) models to their optimal in multi-cloud entities to enhance its security risk detection and prediction measures. Both the integration of the guided and uncontrolled learning approaches as well as the integration of various cloud data and the use of hybrid AI approach allow for the increase in precision and flexibility of threat detection systems. Thus, based on the analysis presented in the paper, it becomes clear that there are certain ways of applying AI to identify both known and newly formed threats. These AI methods include such approaches as deep learning, reinforcement learning, and anomaly detection. The application of hybrid AI models allows for the successful identification of changes within the dynamic multi-cloud environment.

| KEYWORDS

Hybrid AI, Cybersecurity, Multi-cloud Environments, Threat Prediction, Machine Learning, Deep Learning, Anomaly Detection, Reinforcement Learning, Data Fusion, Cloud Security.

| ARTICLE INFORMATION

ACCEPTED: 01 May 2026 **PUBLISHED:** 22 June 2026 **DOI:** 10.32996/fcsai.2026.5.9.3

1. Introduction

Multi-cloud infrastructures integrating services of AWS, Microsoft Azure, and Google Cloud, and commonly on premises, are becoming more popular among enterprises in the United States. Even though this architecture has simplified the process of scaling and has enabled the systems to be more resilient, it has also complicated the process of monitoring security and has

expanded the attack surface. Existing security logs, identity systems, and access controls are not standardized on cloud providers resulting in visibility gaps and slow threat detection. Today, cloud computing has emerged as a disruptive technology that has led to a revolution, not only in the domain of information technology, but also in other domains across the globe. The current situation is viewed to continue in such a way as there continues to be a rising demand for the use of scalable and inexpensive infrastructure services providing quick access to applications [1]. It was the pervasive nature of the multi-cloud environment that brought about a revolution within the organizations through their IT infrastructures, which provided benefits like flexibility and scalability among others. Such conditions in which organizations exploit the services of various cloud providers offer a more multifaceted attack surface that can hardly be handled using conventional cybersecurity methods. The different security measures in place by each provider, and the same weaknesses they may contain would vary and the environment of these providers are constantly changing by different factors like frequent reconfiguration, changing network layout and different data access which makes it even harder to identify threats [2].Traditional security practices, such as firewalls and intrusion detection systems, are typically not sufficient in the multi-cloud environment due to high changes and the varied nature of the cloud services that require them to change swiftly. Moreover, these classical systems continue to base their security with the use of static rules and signatures, which are outdated and useless against the continuously evolving threat environment .The stronger is the need to apply to the integration more sophisticated technologies that include, but are not limited to artificial intelligence (AI) to enhance detection, prediction, and even threat mitigation.AI, in particular, machine learning (ML), has a vast potential in addressing the security issue, which is extremely complicated and irritating in multi-cloud systems. This AI could be deployed to handle vast volumes of data produced by the cloud-based and security platforms, thus detecting any anomalies and patterns that would signal that a possible attack may occur. Yet it is not clear whether following AI-based models would be sufficient for dealing with the dynamic and distributed nature of such environments. Here again, a hybrid approach is called for, i.e., employing various AI methods at once, which is very promising [3]. By incorporating various methods such as supervised learning, unsupervised learning and reinforcement learning, hybrid models can provide threat detection systems not only that are robust but also adaptable. Such models would be at a position to anticipate the already-known threats as well as the new ones. Its capability is based on the previous data besides its capacity to identify new and previously undetermined attack patterns. Regarding the multi-cloud environment, it is reported that the hybrid AI models can become an evolver and adaptor, which can utilize its predictive capacities and simultaneously reduce the risk of the security breach. Multi-cloud optimization technology is the latest innovation in the field of cloud computing for enterprises where through its application it has been possible to overcome the strategic limitations that were faced in the case of using only one cloud provider. It uses the concept of heterogeneity as a strategy strength. Through this approach, it is possible to go beyond the boundaries set by each cloud provider and use different skills and prices offered in diverse locations [4]. The paper that seeks to show how AI can be used for the purpose of cloud security discusses different types of AI algorithms.

2. Background and Motivation

To gain higher flexibility, reduced costs, and remote work, contemporary companies are shifting their services to the cloud at an extremely rapid rate. Due to this pattern, it is typical to see that organizations are typically provided with multi-cloud environments where their services are hosted across multiple cloud environments such as AWS, Microsoft Azure, and Google Cloud. This strategy is good at improving performance, but it results in multifaceted and complex security problems.

Cloud security takes a crucial aspect when companies are quickly moving towards cloud-based architectures to ensure that they get the maximum benefits of scalability, efficiency, and innovation. This chapter provides a detailed discussion of cloud security, the major concepts, new threats, and the progressive defense measures that are necessary to ensure the security of cloud assets. It brings up issues that would be complex, including adaptive identity and access management (IAM), sophisticated encryption techniques, and network security strategies. The critical discussion of the shared responsibility model offers an insight into the subject of accountability by suggesting the distribution of security responsibilities between customers and cloud service providers. Examples of real cloud security attacks are compared to identify areas where security measures are weak, modes of attack, and the significance of the layered defense model [5].

To address these problems, firms are adopting hybrid cybersecurity that is a combination of traditional security practices and innovative technologies like artificial intelligence (AI). AI-based security models have the capability to process enormous volumes of data in the cloud and detect unusual activity and predict the danger that may lead to harm. In addition, such models can learn about its past attack cases, and it can upgrade continuously, thus, they will be more effective after some time.

AI is the central figure that unites the whole security monitoring system in the case of multi-cloud. It collects data across a variety of cloud environments, identifies the points of vulnerability, and notifies the security personnel within a short period of time. The AI-based prediction turns out to be an important element of the safety of the business processes, classified

information, and the confidence of the customers as the threats continue evolving at an extremely rapid pace [6].

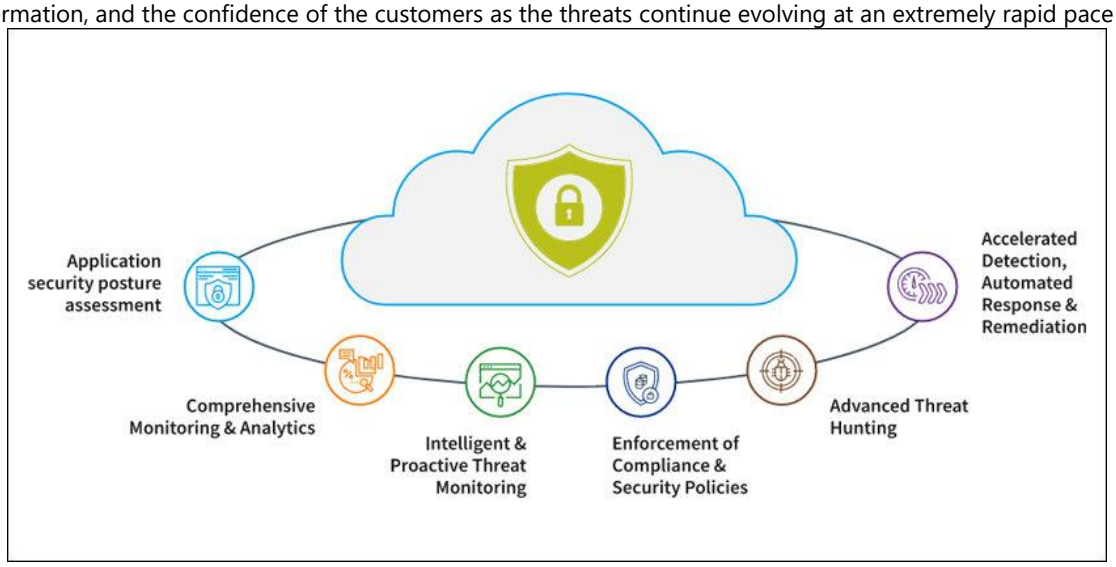

Fig 01: Multi-cloud-management services.

AI and machine learning technologies have proven to be useful in the implementation of cybersecurity measures in a major step. The anomaly detection, through the IDS and through the assessment of threat intelligence, is one of the key fields. Even though different classical AI models can hardly handle the heterogeneity and constant transformation of multi-cloud infrastructure, hybrid models incorporate different AI methods to enhance the scalability, flexibility, and accuracy of the predictions of threats are under consideration.

The initial point of the article is the importance of threat detection in the secure operation of environments of multi-clouds which are becoming more complex due to the decision of companies to use such platforms as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). When discussing the pros and cons of traditional security tools, such as firewalls and intrusion detection systems, the article is very clear on stating that these tools cannot be used in cloud-native infrastructures [7].

The chapter discusses the next-gen practices like Artificial Intelligence (AI)-powered analytics, Machine Learning (ML), User and Entity Behavior Analytics (UEBA), Zero Trust Architecture (ZTA), and Extended Detection and Response (XDR) which are underway implementation.

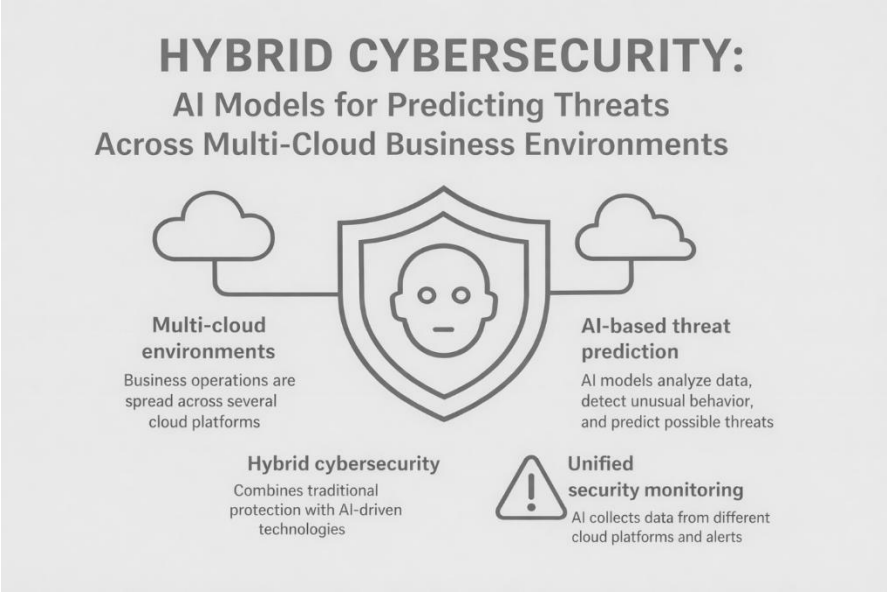

Fig 02: Hybrid Cybersecurity Diagram

3. Hybrid AI Models for Threat Prediction

The hybrid AI models are types of AI models, including deep learning, decision trees, and rule-based systems, that combine to form stronger and more generalized solutions. This type of hybrid models can be also extended to the multi-cloud environment since supervised and unsupervised type of learning can be utilized to detect and predict possible threats by means of past-based data and real- time surveillance. Supervised Learning: These algorithms of supervised learning which are the neural networks as well as the support vectors machine (SVM) are applied to the labeled data to make the predictions as to the eventual outcome. Supervised learning can be used to detect familiar attacks, and the potential security breach can be classified in the case of cybersecurity [8].

The cybersecurity trust model provides a dynamic model for analyzing the trustworthiness of cloud service providers, whereas the multi-risk protection mechanism considers different kinds of risks, including insider risks and data leakage in the context of the layered model framework. Security of information is enhanced further through anomaly detections, intrusion detections, and encryption techniques. Our approach involves the creation of a simulation model and the implementation of the model based on previous real-world experiences in data transmissions. Throughput, latency, and risk detection accuracy will be used as measures of effectiveness.

Unsupervised Learning: By allowing an AI model to recognize new or unknown damage without informing them about the attack patterns, unsupervised learning, such as clustering or anomaly detection, plays a vital role in multi-cloud environments as many different types of threats may happen in this case[9].

Reinforcement Learning: The reinforcement Learning may be applied to keep perfecting and optimizing security practice founded on learning the atmosphere. This approach is most effective in the case of dynamically multi-cloud systems, where the threat space is going to be in a dynamic state of flux.

Such combinations of the threats lead to the hybrid models providing a more stretchy and responsive method of threat prediction and mitigation, especially to the rather complex setting which is a multi-cloud one.

4. Data Fusion and Threat Intelligence

The other major element of hybrid AI models in multi-cloud cybersecurity is data fusion. Threat intelligence platforms and internal security solutions current with information provided by various providers of cloud services, along with various other sources, means that data aggregation and analysis are essential to precise threat anticipation. A hybrid AI System can have a comprehensive picture of the system and can better identify possible threats. Cross-cloud attack vectors can also be identified through this approach, and a more detailed understanding of the security situation is gained [10].

5. Implementation of Hybrid AI in Multi-Cloud Security

To successfully apply the hybrid AI models to multi-cloud systems, an organization should address a variety of issues, such as data gathering, model training, and threat monitoring within real time. Introduction of AI into the current security systems should be in phases to reduce the interruption effect and to ensure that during the implementation, the system has an ability to learn and evolve progressively [11].

Data Collection: Multiple cloud sites should be used to continuously gather data, which will be presented to AI models to ensure they have all the correct and up-to-date information. Such data can comprise network traffic, access logs, authentication logs and threat intelligence feeds.

Model Training: AI models need to be trained with large datasets that include most of the types of attacks. The training must be conducted in a safe place, and models should be constantly updated to describe the emerging threats.

Real-Time Monitoring: Hybrid AI models can be combined with real time monitoring tools to identify threats when they occur and act. The AI system will be able to offer automatic reactions, e.g. blocking suspicious traffic or alerting security personnel.

6. Challenges and Future Directions

Although the concept of hybrid AI models suggests a beneficial perspective, there exist several practical issues in the field of application such as the mismatch of multi-cloud environments, data privacy, and the necessity of the constant retraining of models. Moreover, there will be privacy and regulatory risks (when the volume of data is high) and the industry with very strict data protection regulations.

Fig 03: AI in Cybersecurity: The Comprehensive Guide to Modern Security

Future research should focus on improving the efficiency and accuracy of hybrid AI models, developing more effective data fusion techniques, and addressing privacy and regulatory issues. Additionally, the application of explainable AI (XAI) could help increase trust in AI-driven cybersecurity systems by providing clear insights into decision-making processes [12].

7.Key Statistics Cloud / Multi-Cloud / Hybrid Security

Around 81% of companies report using multi-cloud strategies. ~80% of organizations experienced at least one cloud security breach over the past year.

In a 2023 survey by one major vendor, 39% of businesses said they had a cloud environment data breach in the prior year up from 35% in 2022.

Thales Cyber Security Solutions

Human error / misconfiguration remains a leading cause: in many reports, over 50% of cloud data breaches are traced to human error / misconfiguration.

Thales Cyber Security Solutions

On the defenses (security posture) side: only 56% of organizations said they struggle to secure data across multi-cloud environments showing managing multi-cloud security remains a major headache. Regarding resource use: among cloud workloads, roughly 45% use containerization. Cost of breach: average cost of a cloud security breach for an organization is often cited around US$4.4 million.

Year	Multi-Cloud Adoption (%)	Organizations with Cloud Breach (%)	Misconfiguration-caused Breaches (%)
2021	65	30	45
2022	70	35	48
2023	75	39	50
2024	78	42	52
2025	81	45	55

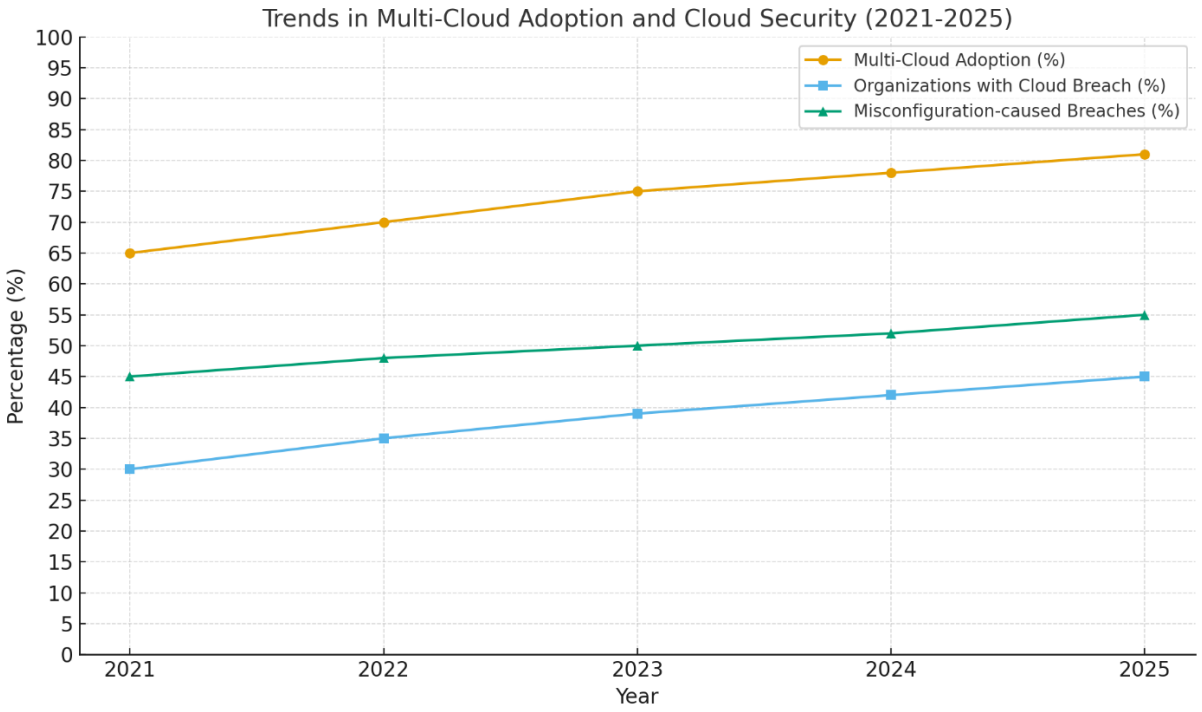

Fig 04: Trends in multi cloud adaptation

8.Future directions:

Federated Learning

AI models are trained across multiple cloud environments without transferring raw data.

This ensures data privacy because sensitive information stays local.

Example: Banks can collaboratively train fraud detection models without sharing customer data.

Real-Time Threat Intelligence Integration

AI systems continuously consume live threat feeds (from hackers, malware reports, etc.).

Models update automatically, allowing faster detection of emerging threats.

Example: A cloud security platform detects new ransomware patterns instantly.

Self-Healing Clouds

AI systems automatically respond to detected threats without human intervention.

Can isolate compromised systems, patch vulnerabilities, or reconfigure resources.

Example: If a server shows unusual activity, the system isolates it and applies fixes automatically.

Explainable AI (XAI)

AI provides clear, interpretable explanations for its decisions.

Help security teams understand why a threat was flagged, improving trust and faster decision-making.

Example: Instead of just labeling traffic as malicious, the AI highlights suspicious IP patterns or file behaviors.

09.Multi-Cloud vs Hybrid-Cloud (Comparison)

Feature	Uses multiple public cloud providers	Hybrid-Cloud
Definition	Public clouds only	Combines private cloud + public cloud
Cloud type	Avoid vendor lock-in	Public and private clouds
Main purpose	Spread across different public clouds	Balance security and scalability
Data location	High flexibility in choosing services	Sensitive data kept in private cloud
Flexibility	Spread across different public clouds	High control over critical workloads
Security	Depends on each provider	Strong control over sensitive data
Complexity	High management complexity	High integration complexity
Example	AWS + Azure + Google Cloud	On-premises data center + AWS

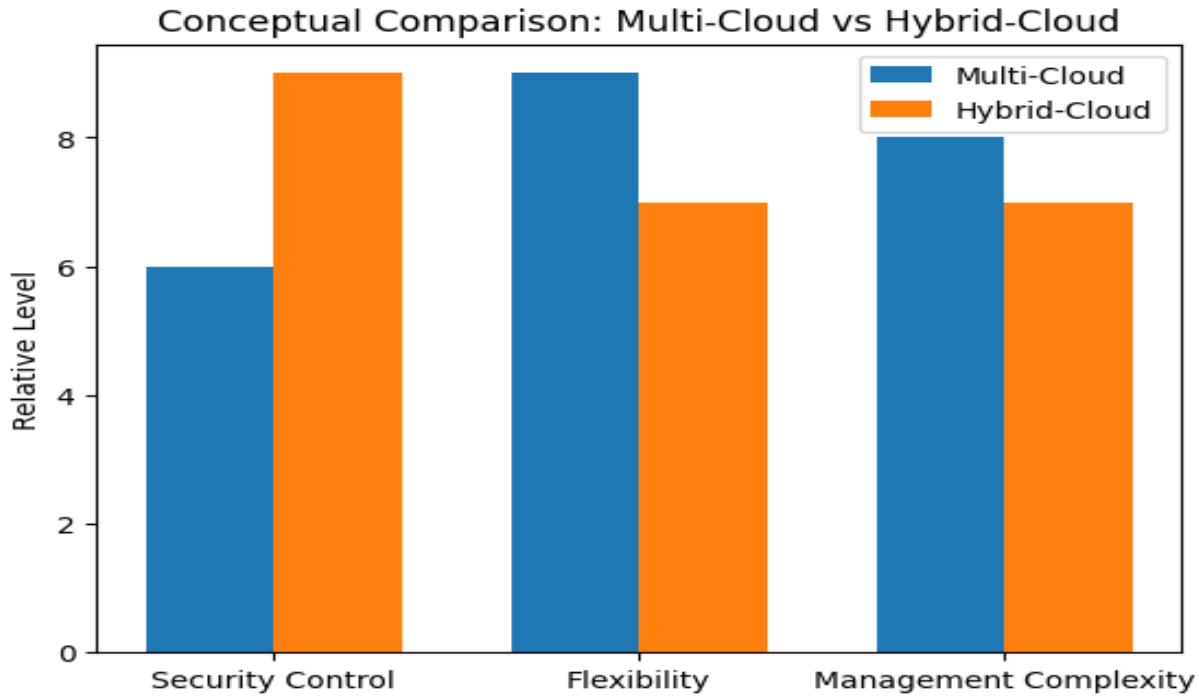

Fig 05: Multi-Cloud vs Hybrid-Cloud.

10. Conclusion:

In conclusion, hybrid cybersecurity frameworks powered by AI across multi-cloud business environments are redefining how organizations manage and mitigate cyber threats. By incorporating federated learning, organizations can collaboratively enhance threat detection without compromising data privacy, enabling secure cross-cloud intelligence sharing. The integration of real-time threat intelligence ensures that security models continuously adapt to emerging and sophisticated cyber-attacks, while self-healing cloud systems provide automated, rapid remediation to reduce operational downtime and human intervention. Explainable AI (XAI) further strengthens these frameworks by offering transparency and actionable insights, building trust in AI-driven security decisions. Looking ahead, the convergence of AI with multi-cloud architecture promises not only more resilient and adaptive cybersecurity but also a strategic advantage in managing risk, ensuring compliance, and driving innovation. As cyber threats grow in complexity and scale, AI-enabled hybrid cybersecurity will be a critical pillar for secure, agile, and future-ready business operations.

Acknowledgement: we would like to express my sincere gratitude to my teacher/supervisor for their valuable guidance, constructive suggestions, and continuous support throughout the preparation of this paper. We are also thankful to all those who directly or indirectly contributed to the completion of this work.

Artificial intelligence policy: we have some minor assistance for the paper's betterment, and we hereby declare that there are no conflicts with any other organization

References

[1] Bayzid, L. H., Kar, T. S., Islam, M. T., Islam, M. S., & Ahmed, F. (2025). Defending the Distributed Skies: A Comprehensive Literature Review of the Arena of Multi-Cloud Environment. Future Internet, 17(12), 548.

[2] Khan, M. I. (2025). Big Data Driven Cyber Threat Intelligence Framework for US Critical Infrastructure Protection. Asian Journal of Research in Computer Science, 18(12), 42-54.

[3] Sudhakar, G., Chandra Shekhar Rao, V., Sunitha, M., Pulipati, V., & Santhosh Kumar, R. (2025). Hybrid AI-based threat prediction and mitigation framework for securing cloud storage. The European Physical Journal Plus, 140(10), 1-26.

[4] Poka, V. (2025). Multi-Cloud Optimization: Orchestrating Workloads Across Heterogeneous Cloud Environments. Journal of Information Systems Engineering and Management, 10(62s), 10-52783.

[5] Shanmugaraja, P., & Sai Senthil Ganapathy, V. (2025, March). Enhancing Advanced Cloud Security Measures in Cloud Environments. In Doctoral Symposium on Computational Intelligence (pp. 381-393). Singapore: Springer Nature Singapore.

[6] Verma, R., & Jailia, M. (2025). A hybrid metaheuristic federated learning approach-based attack detection system for multi-cloud environment. Journal of Cloud Computing, 14(1), 73.

[7] Ali, T. E., & Zoltan, A. D. (2025). Hierarchical Deep Learning for Robust Cybersecurity in Multi-Cloud Healthcare Infrastructures. Engineering, Technology & Applied Science Research, 15(1), 20358-20366.

[8] Kamble, T., Ghuge, M., Jain, R., & Sarbhukan Bodade, V. (2025). Secure data transmission in cloud computing using a cyber-security trust model with multi-risk protection scheme in smart IOT application. Cluster Computing, 28(2), 79.

[9] Farzaan, M. A., Ghanem, M. C., El-Hajjar, A., & Ratnayake, D. N. (2025). AI-powered system for efficient and effective cyber incidents detection and response in cloud environments. IEEE Transactions on Machine Learning in Communications and Networking.

[10] Guo, Y., Liu, Z., Huang, C., Wang, N., Min, H., Guo, W., & Liu, J. (2023). A framework for threat intelligence extraction and fusion. Computers & Security, 132, 103371.

[11] Pachala, S., Rupa, C., & Sumalatha, L. (2021). An improved security and privacy management system for data in multi-cloud environments using a hybrid approach. Evolutionary Intelligence, 14(2), 1117-1133.

[12] Verma, R., & Jailia, M. (2025). A hybrid metaheuristic federated learning approach-based attack detection system for multi-cloud environment. Journal of Cloud Computing, 14(1), 73.