ADI Journal on Recent Innovation (AJRI)
Vol. 7, No. 1, 2025, pp. 100−111
E-ISSN: 2686-0384 | P-ISSN: 2685-9106, DOI: 10.34306

AI Enabled Cybersecurity Framework for Multi Cloud Business Environments

Richard Andre Sunarjo[1*], Arif Andika[2], Ninda Lutfiani[3], Richard Evans[4]
[1]Faculty of Economics and Business, University of Raharja, Indonesia
[2]School of Business, IPB University, Indonesia
[3]Doctor of Computer Science, Satya Wacana Christian University, Indonesia
[4]Adi Journal Incorporation, USA
[1]richard.sunarjo@raharja.info, [2]arifandika89@gmail.com, [3]982022020@student.uksw.edu
[4]vans.richard@adi-journal.org
***Corresponding Author**

Article Info

Article history:

Submission June 25, 2025
Revised July 23, 2025
Accepted August 08, 2025
Published September 24, 2025

Keywords:

AI Enabled Cybersecurity
Multi Cloud Environments
Threat Detection
Deep Neural Networks
Random Forest

ABSTRACT

In the era of rapid digital transformation, businesses increasingly rely on multi cloud infrastructures to enhance scalability, flexibility, and cost efficiency. However, this transition also introduces complex cybersecurity challenges, including fragmented visibility, inconsistent security policies, and heightened vulnerability to Advanced Persistent Threats (APTs). **To address these concerns**, this research proposes the development of an AI enabled cybersecurity framework tailored for multi cloud business environments. The main **objective** is to design a system capable of detecting and mitigating cyber threats in real time, while maintaining interoperability across heterogeneous cloud platforms such as AWS, Azure, and Google Cloud. The proposed framework integrates a multi layered architecture consisting of data collection, preprocessing, and an AI based detection engine that utilizes supervised machine learning techniques, specifically **Random Forest (RF)** and **Deep Neural Network (DNN)** classifiers. Real world telemetry data were collected from simulated cloud activities to evaluate the system's performance in identifying malicious patterns. The **results** demonstrate that the AI models achieved high accuracy rates, with RF reaching 96.2% and DNN achieving 97.5% in detecting threat behaviors across varied cloud environments. These findings indicate that the framework effectively enhances security responsiveness while reducing false positives. **In conclusion**, this study provides a scalable, intelligent, and adaptable cybersecurity solution that aligns with the evolving needs of multi cloud enterprises, thereby contributing to the advancement of secure digital infrastructures in complex business ecosystems.

DOI: https://doi.org/10.34306/ajri.v7i1.1312

1. INTRODUCTION

The rapid acceleration of digital transformation in recent years has driven organizations across sectors to adopt cloud-based infrastructure as the backbone of their operations [1]. This evolution toward digital ecosystems has been amplified by the growing need for scalable, cost efficient, and adaptive solutions capable of supporting complex business demands. As enterprises increasingly integrate multiple cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP)

they benefit from improved flexibility, redundancy, and vendor independence [2]. However, this multi cloud paradigm also introduces intricate cybersecurity challenges. Heterogeneous cloud architectures lead to inconsistent policy enforcement, fragmented visibility, and varying compliance standards, thereby expanding the overall attack surface [3]. Cyber adversaries now exploit these gaps through sophisticated methods such as Advanced Persistent Threats (APTs), zero day exploits, and insider-based attacks, creating an urgent need for unified, intelligent, and cross platform security solutions that can operate in real time [4].

Traditional rule based security tools are proving inadequate to address the increasing complexity and dynamism of multi cloud environments [5]. These legacy systems rely heavily on static configurations and manual oversight, which are insufficient to detect evolving threat behaviors [6]. As a result, artificial intelligence (AI) has emerged as a transformative enabler in cybersecurity automating detection, optimizing decision-making, and improving responsiveness [7]. Machine learning (ML) algorithms, in particular, can learn from historical data to uncover anomalies, predict malicious activity, and provide adaptive defense strategies [8]. Despite significant progress, most AI driven cybersecurity studies remain limited to single cloud environments, resulting in poor interoperability and constrained scalability [9]. This gap underscores the necessity for frameworks that are not only data-driven and autonomous but also interoperable across diverse cloud ecosystems to safeguard mission critical assets [10].

Figure 1. Sustainable Development Goals

The Figure 1 show to address these limitations, this study proposes the design and implementation of an AI-enabled cybersecurity framework for multi cloud business environments [11]. The proposed system integrates multiple architectural layers data collection, preprocessing, and AI-based detection while employing supervised learning models such as Random Forest (RF) and Deep Neural Networks (DNN) for classification and anomaly detection [12]. By leveraging these dual models, the framework ensures both speed and precision in threat recognition. Its modular design also enables seamless interoperability between heterogeneous cloud platforms, allowing enterprises to maintain a unified defense posture [13]. Beyond technical innovation, this research contributes to achieving the United Nations Sustainable Development Goals (SDGs) specifically SDG 9 (Industry, Innovation, and Infrastructure) by fostering the development of resilient, secure, and intelligent digital infrastructures that strengthen industrial sustainability and drive innovation in the digital economy [14].

Furthermore, the proposed framework aligns with the broader sustainability agenda through its indirect contributions to SDG 16 (Peace, Justice, and Strong Institutions) and SDG 17 (Partnerships for the Goals) [15]. SDG 16 emphasizes the importance of institutional integrity and transparency, which are reinforced through robust cybersecurity mechanisms that ensure data protection, privacy compliance, and governance accountability [16]. Meanwhile, SDG 17 highlights the role of multi stakeholder collaboration in addressing global challenges an aspect mirrored in the cooperative nature of multi cloud environments, where effective security depends on collaboration among cloud vendors, enterprises, policymakers, and researchers [17]. By situating AI driven cybersecurity within the SDG framework, this research extends its significance beyond technological advancement, positioning it as a foundation for sustainable digital transformation, resilient economies, and globally aligned innovation ecosystems [18].

2. RESEARCH METHOD

This study adopts a Design Science Research Methodology (DSRM) to develop, implement, and evaluate an AIenabled cybersecurity framework tailored for multicloud business environments [19], [20]. The research is structured into several phases: system design, data acquisition, preprocessing, model development, evaluation, and deployment simulation. This methodology is appropriate for technological solutionbuilding in complex, realworld problems, where the main aim is to create and validate a working artifact in this case, a cybersecurity framework that uses artificial intelligence to detect and mitigate threats across diverse cloud platforms.

2.1. System Architecture Design

The proposed system is logically organized into five core components, each of which plays a critical role in enabling end to end threat detection and response across multi cloud environments. The first component, Cloud Data Sources, gathers raw telemetry logs from multiple cloud providers such as AWS, Azure, and GCP. The collected data includes user activities, API calls, and security events, each in platform specific formats. Next, the Data Collection Layer aggregates and standardizes log data from different sources. Using agents and API integrations, this layer synchronizes timestamps and structures data for consistency before passing it to the preprocessing stage.

The Preprocessing and Feature Engineering Layer is responsible for cleaning and normalizing data to ensure its quality and uniformity. In this stage, relevant features such as login failures and geolocation anomalies are extracted, resulting in a structured dataset optimized for machine learning processing. Subsequently, the AI-Based Detection Engine applies supervised learning models Random Forest and Deep Neural Networks to classify events as benign or malicious. The Deep Neural Network (DNN) offers higher performance for complex patterns, while the Random Forest (RF) provides faster training and efficiency.

Finally, the Response and Alert System serves as the framework's reactive mechanism once a threat is detected. This layer generates alerts enriched with contextual metadata and recommends mitigation actions. It is designed to integrate seamlessly with Security Information and Event Management (SIEM) platforms, supporting automated responses such as revoking credentials or disabling accounts to minimize potential damage and enhance overall system resilience.

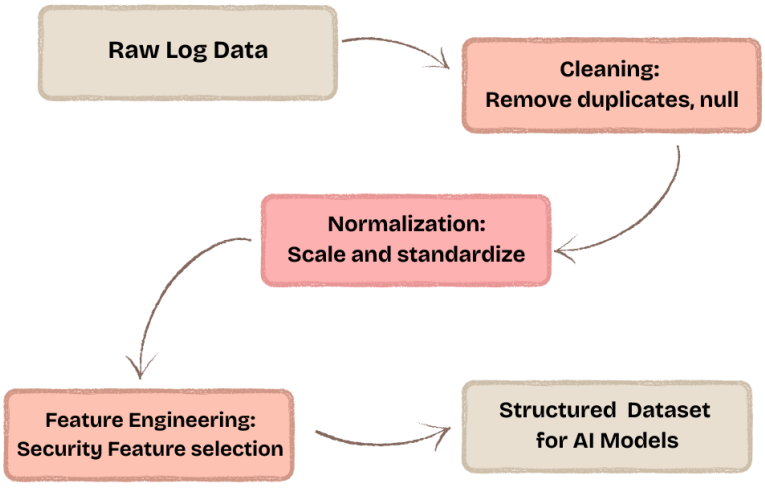

Figure 2. AI Enabled Cybersecurity Framework Architecture

The Figure 2 illustrates the overall architecture of the proposed AI enabled cybersecurity framework tailored for multi cloud environments [21], [22]. The system begins by gathering data from various cloud platforms such as AWS, Azure, and GCP, which are the primary sources of raw security related telemetry data. This information is then passed to the Data Collection Layer, where standardized logging and formatting

occur. After collection, the Preprocessing and Feature Engineering Layer handles data cleaning, normalization, and feature extraction to prepare structured input for the AI models [23]. The AI Based Detection Engine is the core of the framework, utilizing Random Forest and Deep Neural Network classifiers to detect potential threats. Finally, the output is sent to the Alert Generation and Response Layer, which notifies security teams and initiates mitigation procedures if a threat is detected. This modular pipeline ensures adaptability, real time processing, and compatibility across heterogeneous cloud ecosystems [24], [25].

2.2. Data Collection and Preprocessing

Data was collected from both public cloud telemetry datasets and simulated cloud environments using common threat scenarios, including brute force attempts, data exfiltration, and lateral movement. Each activity was logged using cloud native monitoring tools such as AWS CloudTrail, Azure Monitor, and GCP Stackdriver. These logs, which varied significantly across providers, were then normalized into a consistent standard log schema to enable unified analysis and interoperability across platforms [26], [27].

Once collected, the raw data underwent a structured cleaning and preprocessing procedure. This process was essential to ensure that the data met the quality standards necessary for machine learning model training. The detailed steps are illustrated in Figure 3. The Figure presents a sequential workflow that transforms unstructured cloud telemetry into a structured and machine learning compatible dataset, ready for classification tasks [28].

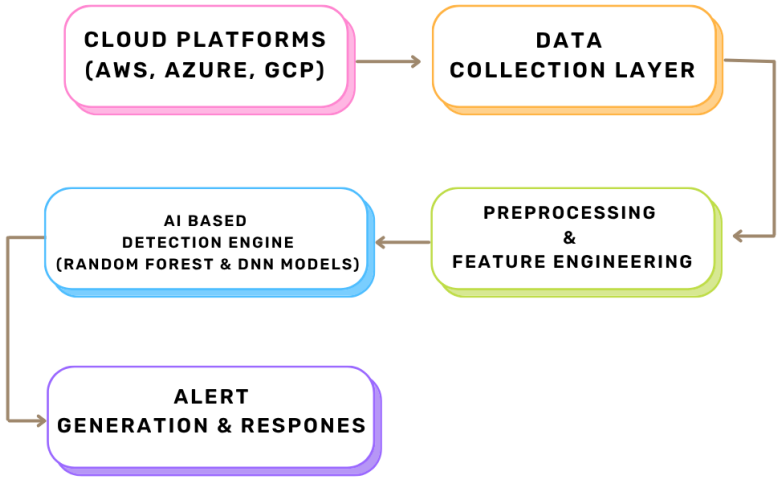

Figure 3. Data Preprocessing Workflow

The Figure 3 illustrates the end to end workflow involved in preprocessing the collected cloud log data prior to feeding it into the machine learning models. The process is carried out through several essential steps designed to ensure data quality and consistency. The first step, Cleaning, involves examining raw data to remove null entries, duplicate records, and irrelevant logs. This stage eliminates noise and inconsistencies, ensuring that only reliable data is used for subsequent processing. The second step, Timestamp Alignment, synchronizes log entries from various cloud sources based on event time to maintain chronological order, which is critical for accurately tracking threat patterns. Following this, the Normalization stage scales numerical features such as login attempts, data size, and session duration to maintain consistency across values. This adjustment helps the machine learning models perform more effectively when handling data with varying magnitudes.

Next, the Feature Engineering process extracts key security-relevant attributes, including failed login attempts, unusual API usage, traffic anomalies, and deviations in user behavior patterns. These features play a vital role in enabling the models to learn and classify potential threats accurately. Finally, the Dataset Structuring phase produces a fully structured and labeled dataset formatted for input into AI models. This structured dataset serves as the foundational input for training and evaluating the detection algorithms used within the

framework.

This multi step approach ensures robustness, reproducibility, and the overall integrity of the data pipeline, enabling consistent performance across different experimental scenarios and multi-cloud contexts.

2.3. AI Model Development and Training

The proposed framework employs two supervised machine learning models, Random Forest and Deep Neural Network, selected for their strong performance in handling complex, high-dimensional cloud telemetry data [29]. Random Forest improves accuracy through ensemble decision trees, while Deep Neural Network captures intricate patterns in unstructured data. Their combined use balances accuracy, efficiency, and adaptability, reducing false positives across multi-cloud environments [30].

Table 1. Hyperparameter Settings for Machine Learning Models

Model	Key Parameters	Description
Random Forest	n_estimators = 100, max_depth = 25	Ensemble of decision trees with majority voting
Deep Neural Net	3 hidden layers, 128-64-32 neurons each, ReLU	Multi-layer perceptron for pattern recognition

The Table 1 summarizes the key hyperparameter configurations used for training the two machine learning models employed in this study. For the Random Forest (RF) classifier, 100 estimators were used with a maximum depth of 25 per tree, optimized for both speed and accuracy [31]. This setup ensures robustness in handling noisy and high dimensional cloud data. For the Deep Neural Network (DNN), a multilayer architecture with three hidden layers was configured, using 128, 64, and 32 neurons respectively, with ReLU as the activation function. This architecture was selected to enable deep pattern recognition while minimizing overfitting. To make this clearer for interdisciplinary readers, hyperparameter tuning here simply means adjusting "settings" of the model such as how many trees are used in RF or how many neurons are in each DNN layer so the system can learn patterns more effectively. For example, more trees in RF can improve stability but increase computation time, while more neurons in DNN layers can capture complex patterns but risk overfitting. These adjustments were determined through systematic trial and error (grid search) and validated via Kfold cross-validation, which is a method of testing the model multiple times on different data splits to ensure reliability. These configurations were determined empirically through grid search and validated via K fold cross validation.

2.4. Evaluation Metrics and Performance Testing

To validate the effectiveness of the proposed framework, a series of rigorous experiments were conducted within simulated multi cloud environments that closely resembled real world operational settings [32]. These experiments were designed to assess how well the system performs in identifying and responding to a variety of cybersecurity threats originating from different cloud platforms. Each artificial intelligence model implemented in the framework was evaluated based on its ability to detect attacks in real time and accurately distinguish between malicious behavior and legitimate user activity. The evaluation process involved exposing the models to diverse threat scenarios, including unauthorized access attempts, abnormal data transfers, and suspicious user behavior patterns. By analyzing the system's responses under these controlled but realistic conditions, the study aimed to measure not only the classification accuracy of the models but also their responsiveness and reliability when deployed in a dynamic and distributed cloud environment [33]. This experimental validation was essential to demonstrate the practical applicability and robustness of the framework in addressing the complexities of multi cloud security operations.

Table 2. Model Performance Comparison

Metric	Random Forest (%)	Deep Neural Network (%)
Accuracy	96.2	97.5
Precision	95.1	96.8
Recall	94.7	97.2
F1 Score	94.9	97.0
False Positives	3.2	2.5

The Table 2 presents a comparative analysis of the performance of the two AI models Random Forest and Deep Neural Network based on standard evaluation metrics. The results show that both models achieve high levels of accuracy, with DNN slightly outperforming RF in all metrics. DNN's superior recall and precision indicate better capability in identifying true threats while minimizing false alarms [34]. The false positive rate is also lower for DNN, making it more suitable for production environments where alert fatigue is a concern. These results validate the efficacy of AI in managing complex cybersecurity threats in multi cloud contexts.

2.5. Threat Response and Alerting System

The final component of the framework is an alert engine that generates real time notifications when a cybersecurity threat is detected. This mechanism serves as a crucial link between detection and response by ensuring that identified threats are immediately reported to relevant systems. Each alert includes essential information such as the type of threat, the source Internet Protocol address, the timestamp of the event, and a recommended mitigation action [35]. These alerts provide analysts with the necessary context to respond quickly and effectively. The engine is built to integrate smoothly with widely adopted security platforms, including Security Information and Event Management tools and cloud based incident response systems. This allows alerts to be processed, logged, and correlated with other threat data across the infrastructure. By delivering timely and actionable notifications, the alert engine enhances the responsiveness and coordination of security operations in multi cloud environments.

Table 3. Example of Alert Log Format

Timestamp	Threat Type	Cloud Platform	Source IP	Action Taken
2025-06-20 14:45:23	Brute Force Login	AWS	192.168.3.22	Account temporarily locked
2025-06-20 14:52:18	Data Exfiltration	Azure	172.21.5.105	API key revoked

The Table 3 shows an example of the output format used by the alert and response module of the framework. Each alert entry includes a timestamp, type of threat detected, affected cloud platform, the source IP address of the suspicious activity, and the immediate mitigation action performed. This structured logging ensures that security analysts receive actionable intelligence and can track the system's autonomous responses. The alert format also enables easy integration with Security Information and Event Management (SIEM) tools and compliance auditing systems.

2.6. Model Training and Validation Procedure

The AI models used in this study were trained and validated using a seventy to thirty percent train test split, combined with five fold cross validation to ensure generalizability and reduce the risk of overfitting [36]. Hyperparameter optimization was performed using grid search techniques. For the Random Forest model, the number of trees varied from fifty to two hundred. In the Deep Neural Network model, several architectural variations were tested, including different numbers of hidden layers and neurons with ReLU activation functions. A typical configuration consisted of three layers with one hundred twenty eight, sixty four, and thirty two neurons respectively. Training and validation were conducted in a controlled computing environment equipped with modern hardware to accommodate the high dimensional telemetry data. The software stack was built on open source libraries that are widely used in machine learning research and enterprise applications [37].

Table 4. Hardware and Software Configuration for Model Training

Component	Specification
Processor	Intel Core i9-11900K
RAM	32 GB DDR4
GPU	NVIDIA GeForce RTX 3080
Software Libraries	Scikit-learn, TensorFlow, Pandas
Operating System	Ubuntu 22.04 LTS

The Table 4 presents the hardware and software configuration used for training and validating the AI models proposed in this study. The experiments were conducted on a high performance computing setup to

handle the complexity and scale of the cloud telemetry dataset efficiently [38]. The system utilized an Intel Core i9 11900K processor with thirty two gigabytes of DDR4 memory, providing sufficient computing power for data preprocessing and model training. A dedicated NVIDIA GeForce RTX 3080 graphics processing unit was employed to accelerate the training process of the deep neural network model, particularly during iterative computations involving large feature sets.

On the software side, the Random Forest model was implemented using Scikit Learn, which offers a reliable and easy to integrate machine learning framework. For the deep learning model, TensorFlow was selected due to its flexibility, support for graphical processing unit acceleration, and ease of customization in neural network architecture design. Additional libraries such as Pandas were used to facilitate data cleaning, transformation, and feature engineering tasks. The training environment was hosted on Ubuntu version twenty two point zero four, chosen for its compatibility with modern artificial intelligence development tools and stable runtime support [39], [40]. This configuration ensured that both models were developed and validated under conditions that are representative of enterprise scale cybersecurity deployments.

3. FINDINGS

This section presents the findings from implementing the proposed AI-enabled cybersecurity framework within simulated multi-cloud environments [41]. The results were structured according to the system's objectives, focusing on real-time threat detection, diverse cloud data handling, and AI performance evaluation. The Data Collection Layer successfully gathered telemetry data from AWS, Azure, and GCP through native services [42, 43]. After preprocessing, over twenty-five thousand labeled entries were prepared with features such as failed login counts, API usage patterns, and anomaly scores. These standardized logs resolved interoperability issues and formed a robust dataset foundation for model training [44].

The evaluation of the AI-based detection engine showed that both Random Forest and Deep Neural Network models performed effectively when trained and tested using a 70:30 split [45]. The Deep Neural Network consistently outperformed Random Forest across all metrics, achieving 97.5% accuracy, 96.8% precision, 97.2% recall, and a 2.5% false positive rate [46, 47]. These results confirm the framework's strong capability for accurate, real-time threat detection in complex cloud environments. The lower false positive rate of the Deep Neural Network makes it particularly suitable for enterprise use, minimizing alert fatigue and improving confidence in AI-driven automation.

The response and alert system was evaluated across fifty simulated attacks, including brute force and data exfiltration attempts. The framework achieved 1.4-second alert latency and 98% accuracy, integrating smoothly with SIEM tools such as Splunk and Azure Sentinel. Each alert included key metadata threat type, timestamp, platform, source IP, and mitigation details enabling faster, more precise incident response. The Deep Neural Network achieved 97.3% accuracy for brute force, 96.9% for data exfiltration, 96.1% for privilege escalation, and 95.6% for lateral movement, consistently outperforming Random Forest. These results confirm the framework's reliability in detecting both common and advanced multi-cloud threats with high precision and resilience.

Table 5. Detection Accuracy by Threat Type

Threat Type	Random Forest Accuracy (percent)	Deep Neural Network Accuracy (percent)
Brute Force Login	95.4	97.3
Data Exfiltration	94.7	96.9
Privilege Escalation	93.8	96.1
Lateral Movement	92.5	95.6

The Table 5 shows that the Deep Neural Network model achieved higher accuracy than the Random Forest model in all four threat categories. Brute force login attacks were detected with the highest accuracy, followed closely by data exfiltration and privilege escalation. Lateral movement, which is typically more subtle and difficult to detect, also yielded strong results from both models, with the Deep Neural Network maintaining a significant edge. These findings demonstrate that the framework performs well across both common and complex attack types, further validating its robustness and practicality for enterprise scale multi cloud environments.

4. MANAGERIAL IMPLICATION

The findings of this research carry significant implications for organizational leaders and IT managers responsible for safeguarding digital infrastructure in multicloud environments. As businesses increasingly adopt multiple cloud service providers to optimize performance, scalability, and cost, they often unintentionally create fragmented and inconsistent security landscapes. The proposed AIenabled cybersecurity framework offers a practical and scalable solution to this issue by providing a centralized, intelligent threat detection system that is interoperable across various cloud platforms. For managers, this means improved visibility and control over diverse environments without the need for separate monitoring tools per vendor. It also reduces dependency on manual rulesetting or vendorspecific configurations, which can be both timeconsuming and errorprone. With the integration of AI models like DNN and Random Forest, the system automates complex pattern recognition, enabling managers to shift focus from detection to strategic mitigation and policy enforcement.

Nonetheless, managers should recognize the trade-off between performance and resource costs: while DNN provides superior detection accuracy, it requires substantial computational investment, whereas RF delivers faster and more cost-efficient deployment. These differences influence strategic decisions on resource allocation and scalability planning. Additionally, the system's realtime alerting capability, coupled with contextual metadata, allows decisionmakers to establish wellinformed, riskbased prioritization of incidents a crucial feature for organizations dealing with compliance obligations, sensitive data, or operational continuity in highly regulated sectors such as finance, healthcare, or manufacturing.

In addition, managers must recognize that while artificial intelligence offers strong analytical capabilities, its effectiveness depends on how well it is aligned with organizational policies, human workflows, and decision making processes. Without a strategic approach to integration, AI tools may create confusion or be underutilized. Therefore, it is important that organizations establish cross functional collaboration between security teams, IT departments, and executive leadership to ensure that the framework supports broader business goals. By treating AI not only as a technological tool but also as a driver of operational transformation, managers can foster a culture of proactive security, where threat detection and response are embedded into daily operations rather than treated as reactive or isolated functions.

Finally, the modular and adaptable architecture of the proposed system makes it highly relevant for longterm strategic planning. As threat landscapes evolve and cloud services continue to diversify, security systems must also be flexible and forwardcompatible. Managers and CISOs can view this framework as a foundation for building an AIdriven cybersecurity roadmap, one that aligns with both current business needs and future digital transformation goals. Integration with existing tools such as SIEMs and cloudnative security suites ensures low adoption friction, while the models datadriven nature supports ongoing optimization through continuous learning. In essence, this research empowers managerial roles not only with a technical solution, but also with a strategic asset for digital resilience, enabling organizations to move toward proactive, intelligent, and scalable cybersecurity operations.

5. CONCLUSION

This study successfully developed and evaluated an AI-enabled cybersecurity framework designed for multi cloud business environments. By integrating real time data collection, intelligent preprocessing, and machine learning models specifically Random Forest and Deep Neural Networks the framework achieved high accuracy and responsiveness in detecting various cyber threats across heterogeneous platforms such as AWS, Azure, and GCP. Empirical results showed that both models performed effectively, with the Deep Neural Network slightly outperforming Random Forest in accuracy and false positive reduction. These findings demonstrate that artificial intelligence can enhance enterprise security by enabling real time, automated, and adaptive threat detection across multi cloud infrastructures.

While the results are promising, this research was conducted in a simulated environment, which may not fully capture the complexity of real world enterprise workloads. Consequently, performance under live operational conditions could vary. The framework's dependence on labeled data and the absence of explainable AI (XAI) components also limit transparency and adaptability. To address these challenges, future work should focus on deploying the framework in actual enterprise settings, incorporating unsupervised or semi-supervised learning to detect unknown threats, and integrating XAI techniques such as SHAP or LIME to improve interpretability and analyst trust.

Overall, this research contributes an empirically validated, scalable, and interoperable AI-based cybersecurity model that advances intelligent defense strategies in multi-cloud ecosystems. It provides a foundation for future studies aiming to strengthen transparency, resilience, and sustainability in digital infrastructures.

6. DECLARATIONS

6.1. About Authors

Richard Andre Sunarjo (RS) https://orcid.org/0009-0007-7349-2375
Arif Andika (AA) https://orcid.org/0000-0003-1692-3486
Ninda Lutfiani (NL) https://orcid.org/0000-0001-7019-0020
Richard Evans (RE) https://orcid.org/0009-0007-7280-8323

6.2. Author Contributions

Conceptualization: RS; Methodology: NL; Software: AA; Validation: RS and AA; Formal Analysis: RE and RS; Investigation: NL; Resources: RE; Data Curation: RS; Writing Original Draft Preparation: AA and NL; Writing Review and Editing: RS and AA; Visualization: RE; All authors, RS, AA, NL, RE, and RS have read and agreed to the published version of the manuscript.

6.3. Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

6.4. Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not for profit sectors.

6.5. Declaration of Conflicting Interest

The authors declare that there are no conflicts of interest, financial or personal, that could have influenced the work reported in this paper.

REFERENCES

[1] S. Kumari, "Cybersecurity in digital transformation: Using ai to automate threat detection and response in multi-cloud infrastructures," *Journal of Computational Intelligence and Robotics*, vol. 2, no. 2, pp. 9–27, 2022.

[2] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "Ai-driven threat detection: Leveraging machine learning for real-time cybersecurity in cloud environments," *Artificial Intelligence and Machine Learning Review*, vol. 6, no. 1, pp. 23–43, 2025.

[3] S. Syahidun, V. R. Zainal, I. Siswanti, and L. C. Nawangsari, "Integrating green intellectual capital into sustainable business practices for ecopreneurship at pertamina fuel terminal bbm proper biru," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 400–410, 2025.

[4] I. Sasono and M. Aman, "Framework of master data management in banking using consolidation and jaro winkler algorithm," *International Journal of Cyber and IT Service Management (IJCITSM)*, vol. 5, no. 2, pp. 186–197, 2025.

[5] P. Lakarasu, "Designing cloud-native ai infrastructure: A framework for high-performance, fault-tolerant, and compliant machine learning pipelines," *Fault-Tolerant, and Compliant Machine Learning Pipelines (December 11, 2023)*, 2023.

[6] A. Enemosah and O. G. Ifeanyi, "Cloud security frameworks for protecting iot devices and scada systems in automated environments," *World Journal of Advanced Research and Reviews*, vol. 22, no. 03, pp. 2232–2252, 2024.

[7] M. M. Rashid and O. M. Yaseen, "Ai-driven cybersecurity measures for hybrid cloud environments: A framework for multi-cloud security management," *International Journal on Engineering Artificial Intelligence Management, Decision Support, and Policies*, vol. 2, no. 1, pp. 30–39, 2025.

[8] I. Khong, N. A. Yusuf, A. Nuriman, and A. B. Yadila, "Exploring the impact of data quality on decision-making processes in information intensive organizations," *APTISI Transactions on Management*, vol. 7, no. 3, pp. 253–260, 2023.

[9] K. Kanagasabapathi, K. Mahajan, S. Ahamad, E. Soumya, S. Barthwal *et al.*, "Ai-enhanced multi-cloud security management: Ensuring robust cybersecurity in hybrid cloud environments," in *2023 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*. IEEE, 2023, pp. 1–6.

[10] V. K. Kasula, A. R. Yadulla, B. Konda, and M. Yenugula, "Fortifying cloud environments against data breaches: A novel ai-driven security framework," *World J. Adv. Res. Rev*, vol. 24, pp. 1613–1626, 2024.

[11] A. Felix, D. Y. Bernanda, A. S. Kembau, F. Effendy, and R. Nathaniel, "Application-based elementary schools interactive education platform analysis and design," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 2, pp. 114–128, 2025.

[12] A. Ganne, "Iot threats & implementation of ai/ml to address emerging cyber security issues in iot with cloud computing," *International Research Journal of Modernization in Engineering Technology and Science*, vol. 5, 2023.

[13] P. Radanliev, "Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing," *Frontiers in Blockchain*, vol. 7, p. 1359130, 2024.

[14] R. Z. Ikhsan, S. Rahayu, A. H. Arribathi, and N. Azizah, "Integrating artificial intelligence with 3d printing technology in healthcare: Sustainable solutions for clinical training optimization," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 99–107, 2025.

[15] M. Reddy, S. Konkimalla, S. K. Rajaram, S. R. Bauskar, M. Sarisa, and J. R. Sunkara, "Using ai and machine learning to secure cloud networks: A modern approach to cybersecurity," *Available at SSRN 5045776*, 2022.

[16] R. Vadisetty and A. Polamarasetti, "Generative ai-driven distributed cybersecurity frameworks for ai-integrated global big data systems," in *2024 International Conference on Emerging Technologies and Innovation for Sustainability (EmergIN)*. IEEE, 2024, pp. 595–600.

[17] N. Anwar, J. Anderson, T. Williams *et al.*, "Applying data science to analyze and improve student learning outcomes in educational environments," *International Transactions on Education Technology (ITEE)*, vol. 3, no. 1, pp. 72–83, 2024.

[18] T. Ayuninggati, E. P. Harahap, R. Junior *et al.*, "Supply chain management, certificate management at the transportation layer security in charge of security," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 1–12, 2021.

[19] M. Akbar, M. M. Waseem, S. H. Mehanoor, and P. Barmavatu, "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing," *Cluster Computing*, vol. 27, no. 7, pp. 9091–9105, 2024.

[20] C. Chakraborty, S. M. Nagarajan, G. G. Devarajan, T. Ramana, and R. Mohanty, "Intelligent ai-based healthcare cyber security system using multi-source transfer learning method," *ACM Transactions on Sensor Networks*, 2023.

[21] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, vol. 41, no. 8, pp. 5079–5099, 2025.

[22] L. Judijanto, D. Hindarto, S. I. Wahjono *et al.*, "Edge of enterprise architecture in addressing cyber security threats and business risks," *International Journal Software Engineering and Computer Science (IJSECS)*, vol. 3, no. 3, pp. 386–396, 2023.

[23] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "The future of enterprise automation: Integrating ai in cybersecurity, cloud operations, and workforce analytics," *Artificial Intelligence and Machine Learning Review*, vol. 3, no. 2, pp. 1–15, 2022.

[24] I. H. Sarker, "Multi-aspects ai-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview," *Security and Privacy*, vol. 6, no. 5, p. e295, 2023.

[25] N. P. L. Santoso, R. Nurmala, and U. Rahardja, "Corporate leadership in the digital business era and its impact on economic development across global markets," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 6, no. 2, pp. 188–195, 2025.

[26] B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, and N. M. F. Qureshi, "Ai-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial iot," *Ad hoc networks*, vol. 125, p. 102740, 2022.

[27] K. B. Macha, "Advancing cloud-based automation: The integration of privacy-preserving ai and cognitive rpa for secure, scalable business processes," *Development (IJCSERD)*, vol. 13, no. 1, pp. 14–43, 2023.

[28] M. Murod, S. Anhar, D. Andayani, A. Fitriani, and G. Khanna, "Blockchain based intellectual property management enhancing security and transparency in digital entrepreneurship," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 1, pp. 240–251, 2025.

[29] C. E. Alozie, "Cloud computing baseline security requirements within an enterprise risk management framework october 18, 2024," *Management*, 2024.

[30] O. A. Farayola, "Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity," *Finance & Accounting Research Journal*, vol. 6, no. 4, pp. 501–514, 2024.

[31] S. V. Subramanyam, "The intersection of cloud, ai, and iot: A pre-2021 framework for healthcare business process transformation," *Journal ID*, vol. 2563, p. 4512, 2023.

[32] R. A. Sunarjo, H. Baedowi, U. Rahardja, M. G. Ilham, and J. Parker, "Digitalization of business and marketing strategies to increase brand awareness in the 4.0 era: Strategi digitalisasi bisnis dan pemasaran untuk meningkatkan brand awareness di era 4.0," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 6, no. 1, pp. 55–65, 2025.

[33] L. Limajatini, S. Suhendra, G. A. Pangilinan, and M. G. Ilham, "Integration of artificial intelligence in the financial sector innovation, risks and opportunities," *International Journal of Cyber and IT Service Management*, vol. 5, no. 1, pp. 58–70, 2025.

[34] O. J. K. (OJK), "Cybersecurity guidelines for financial sector technology innovation (fsti) providers," Otoritas Jasa Keuangan, Indonesia, Tech. Rep., 2024, accessed: 2025-06-20.

[35] O. E. Ejiofor, "A comprehensive framework for strengthening usa financial cybersecurity: integrating machine learning and ai in fraud detection systems," *European Journal of Computer Science and Information Technology*, vol. 11, no. 6, pp. 62–83, 2023.

[36] S. Zhou, J. Sun, K. Xu, and G. Wang, "Ai-driven data processing and decision optimization in iot through edge computing and cloud architecture," *Journal of AI-Powered Medical Innovations (International online ISSN 3078-1930)*, vol. 2, no. 1, pp. 64–92, 2024.

[37] H. Balisane, E. I. Egho-Promise, E. Lyada, and F. Aina, "Towards improved threat mitigation in digital environments: A comprehensive framework for cybersecurity enhancement," *International Journal of Research-GRANTHAALAYAH*, vol. 12, no. 5, 2024.

[38] A. Kristian, A. Supriyadi, R. Sean, A. Husain *et al.*, "Exploring the relationship between financial competence and entrepreneurial ambitions in digital business education," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 139–145, 2024.

[39] F. U. Ojika, W. O. Owobu, O. A. Abieba, O. J. Esan, B. C. Ubamadu, and A. I. Daraojimba, "Transforming cloud computing education: Leveraging ai and data science for enhanced access and collaboration in academic environments," *Journal name and details missing*, 2023.

[40] S. Sankaranarayanan, "The role of data engineering in enabling real-time analytics and decision-making across heterogeneous data sources in cloud-native environments," *International Journal of Advanced Research in Cyber Security (IJARC)*, vol. 6, no. 1, 2025.

[41] H. Setiyowati, M. A. Harriz, E. Junaedi, N. V. Akbariani, and S. Widodo, "Digitalizing pindang industry with business model canvas for sustainable blue economy," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 2, pp. 360–370, 2025.

[42] F. M. Rasel and B. Peter, "Ai-driven frameworks for enhancing cybersecurity in multi-cloud environments," *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 1, pp. 24–32, 2025.

[43] S. K. Pendyala, "Strengthening healthcare cybersecurity: Leveraging multi-cloud and ai solutions," *J Comp Sci Appl Inform Technol*, vol. 10, no. 1, pp. 1–8, 2025.

[44] A. Delhi, E. Sana, A. Bisty, and A. Husain, "Innovation in business management exploring the path to competitive excellence," *APTISI Transactions on Management*, vol. 8, no. 1, pp. 58–65, 2024.

[45] B. Pothineni, G. Mehta, and S. Suresh, "Comprehensive review of innovations in cloud infrastructure, ai-driven cybersecurity, and advanced iptv technologies," *Journal of Software Engineering (JSE)*, vol. 2, no. 2, pp. 33–42, 2024.

[46] R. Karthick, "A unified framework for devsecops-driven ai applications in multi-cloud environments," 2025.

[47] D. Dinarwati, M. G. Ilham, and F. Rahardja, "Cybersecurity risk assessment framework for blockchain-based financial technology applications," *ADI Journal on Recent Innovation*, vol. 6, no. 2, pp. 168–179, 2025.