OMANARP INTERNATIONAL JOURNAL OF NATURAL & APPLIED SCI.

https://acadrespub.com/index.php/oijnas

Vol. 2, Issue I, Pp. 16-22; NOV., 2025

PROACTIVE CLOUD RISK MANAGEMENT : AN INTELLIGENT FRAMEWORK LEVERAGING MACHINE LEARNING AND EXPLAINABLE AI

[1]OMOREGIE Dolly Arenvbaguehita [2]OMOROGBE Osasu Harry (PhD); [3]EDUJE, Anthony Ighoakpo; [4]AMOFORITSE, Fortune Ighotuweyin & [5]Kingsley Chiwuike Ukaoha PhD.

Department of Cyber Security, Igbinedion University, Okada. Edo State, Nigeria; Department of Computer Science and Information Technology, Igbinedion University, Okada.; Department of Computer Science and Information Technology, Igbinedion University, Okada. Edo State, Nigeria. Department of Cyber Security and ICT Unit, Igbinedion University, Okada. Edo State, Nigeria; Dean, College of Science and Computing. WIGWE University, Rivers State, Nigeria

https://orcid.org/0000-0002-6864-3665

Email: omorogbe.harry@iuokada.edu.ng; omoregie.dolly@iuokada.edu.ng; dujeit@yahoo.com; amoforitse.fortune@iuokada.edu.ng; kingsley.ukaoha@wigwe.edu.ng

ARTICLE INFO

Received Date: 25th OCT, 2025
Date Revised Received: 27th OCT, 2025
Accepted Date: 7th NOV, 2025
Published Date: 10th Nov. 2025

Citation: Omoregie, D. A..et al (2025);Proactive Cloud Risk Management: An Intelligent Framework Leveraging Machine Learning and Explainable AI . Vol.2, Issues I Omanarp Int. J NAS: Nov.2025. Pp.16- 22

ABSTRACT

Cloud computing has transformed the management of data and applications by enabling scalability, flexibility, and cost-efficiency across organizational infrastructures. However, it simultaneously introduces new and complex security challenges, including data breaches, configuration vulnerabilities, and unauthorized access. This study presents the design and implementation of an intelligent, machine learning–driven risk assessment framework for cloud-based systems that proactively identifies, evaluates, and mitigates cybersecurity threats. The framework employs supervised and unsupervised learning techniques such as Random Forest, Support Vector Machines, and Long Short-Term Memory (LSTM) networks to detect anomalies and predict risk levels. Data were sourced from benchmark datasets (e.g., UNSW-NB15, CICIDS2017) and synthetic cloud simulations to ensure robustness and realism. Results from experimental evaluations demonstrate that the proposed model achieves high detection accuracy and adaptability, outperforming conventional static risk assessment techniques. By integrating explainable AI (XAI) methods such as SHAP and LIME, the framework enhances interpretability and compliance alignment with standards like NIST SP 800-53 and ISO/IEC 27001. The findings contribute to advancing proactive, automated, and intelligent risk management strategies for secure and resilient cloud computing environments.

Keywords: Cloud Computing; Machine Learning; Risk Assessment Framework; Cybersecurity; Anomaly Detection; Explainable AI (XAI);

Introduction

Cloud computing has become a cornerstone of digital transformation, empowering organizations with on-demand access to computing power, storage, and applications through virtualized infrastructures. Major providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) dominate this ecosystem, enabling flexible, cost-effective, and scalable service delivery (Hashizume et al., 2021; Xu et al., 2022; Hamid & Rahman, 2025). Despite these advantages, the dynamic, multi-tenant, and distributed nature of cloud environments introduces complex security risks, including data breaches, misconfigurations, and insider threats (Fan et al., 2023; Al-Amin et al., 2023).

Traditional security models typically rule-based and reactive struggle to detect advanced persistent threats (APTs) and zero-day attacks in real time (Saha & Roy, 2022; Bhadauria & Soni, 2021). As organizations increasingly depend on multi-cloud and hybrid infrastructures, the demand for proactive, intelligent, and adaptive risk management grows (Calzarossa et al., 2025). Machine learning (ML) has emerged as a viable approach to this challenge, offering the capacity to analyze massive cloud data streams, detect anomalies, and predict threats dynamically (Kumar & Goudar, 2021; Liu et al., 2023).

Recent studies have demonstrated ML's success in intrusion detection, threat forecasting, and behavioral analytics (Shah & Patel, 2022; Nerella et al., 2025). However, current implementations often lack interpretability, scalability, and integration with compliance standards like ISO/IEC 27001 or NIST SP 800-53 (Zhou & Zhang, 2024; Awodele et al., 2024). Hence, there is a need for an integrated ML-driven framework that supports real-time cloud risk assessment, aligns with regulatory requirements, and provides transparent, explainable outputs to security analysts. This research aims to fill this gap by developing a comprehensive, adaptive, and interpretable Machine Learning–Driven Cloud Risk Assessment Framework (ML-CRAF).

Statement of the Research Problem

The widespread adoption of cloud computing has fundamentally redefined data management and service delivery across industries. However, this shift has also increased exposure to sophisticated cybersecurity threats, including data breaches, insider attacks, and system misconfigurations (Al-Amin et al., 2023; Hamid & Rahman, 2025). Traditional risk assessment approaches—primarily manual, rule-based, or static—struggle to cope with the volume, velocity, and variability of modern cloud data (Saha & Roy, 2022). These methods often lack real-time adaptability, interpretability, and the ability to detect zero-day or multi-stage attacks (Liu et al., 2023; Nerella et al., 2025).

Moreover, as cloud systems become more decentralized and dynamic, existing tools fail to integrate multiple data sources effectively or align with compliance frameworks like ISO/IEC 27001, NIST SP 800-53, and CSA Cloud Controls Matrix (Zhou & Zhang, 2024). This limits their practical use for continuous risk monitoring and automated decision-making in hybrid and multi-cloud infrastructures (Calzarossa et al., 2025).

Consequently, there is a critical need for an intelligent, adaptive, and explainable machine learning–driven framework capable of automating risk detection, classification, and prioritization in real-time. Such a framework should not only identify anomalous behaviors but also provide actionable insights to help security analysts mitigate emerging threats efficiently and ensure compliance with global security standards.

Research Aim

The primary aim of this study is to design, implement, and evaluate a Machine Learning–Driven Cloud Risk Assessment Framework (ML-CRAF) that autonomously identifies, assesses, and prioritizes potential security threats in cloud-based systems.

Research Objectives

To achieve this aim, the study will pursue the following objectives:

1. To identify and analyze existing limitations in conventional cloud risk assessment methodologies.
2. To design and develop a multi-layered machine learning framework (ML-CRAF) that integrates supervised, unsupervised, and deep learning models for comprehensive risk analysis.
3. To implement the proposed framework using public and simulated cloud datasets (e.g., UNSW-NB15, CICIDS2017, and Azure/AWS logs).
4. To evaluate the framework's performance using standard metrics such as accuracy, precision, recall, F1-score, and AUC.
5. To assess the interpretability and compliance readiness of the framework through Explainable AI (XAI) techniques such as SHAP and LIME.
6. To compare the framework's performance with traditional risk assessment approaches to determine efficiency and scalability improvements.

Literature Review

This section reviews relevant literature on cloud computing security, risk assessment methodologies, and the integration of machine learning in cloud-based threat detection. It also highlights existing research gaps that this study addresses. The literature review is organized into four main sub-sections: (1) cloud security and its challenges, (2) traditional and modern risk assessment frameworks, (3) machine learning techniques for risk analysis, and (4) explainable AI for interpretability in cybersecurity.

Cloud Security and Challenges

Cloud computing has evolved into the backbone of modern digital infrastructure, providing on-demand access to computing resources through scalable, distributed architectures. However, its open and dynamic nature exposes it to numerous security threats, such as data breaches, insecure APIs, denial-of-service attacks, and insider threats (Hamid & Rahman, 2025; Saha & Roy, 2022). Studies by Awodele et al. (2024) and Al-Amin et al. (2023) emphasize that these vulnerabilities are intensified by multi-tenancy, virtualization, and the shared responsibility model that blurs accountability boundaries between cloud providers and users.

Recent research has also pointed out that as organizations migrate toward hybrid and multi-cloud architectures, the complexity of monitoring and securing these environments increases exponentially (Nerella et al., 2025; Calzarossa et al., 2025). These challenges necessitate continuous, data-driven risk assessment methods capable of responding to evolving threats in real time rather than relying on periodic audits or manual inspections.

Traditional and Modern Risk Assessment Frameworks

Traditional risk assessment frameworks, including NIST SP 800-53, ISO/IEC 27001, and the CSA Cloud Controls Matrix, provide structured approaches for identifying and mitigating risks (Zhou & Zhang, 2024). However, these standards rely heavily on qualitative scoring systems that are subjective and reactive, often failing to adapt to dynamic threat landscapes (Kumar & Goudar, 2021).

In response, modern research emphasizes the integration of automation and machine intelligence to enhance predictive capabilities. For instance, Shaukat et al. (2023) proposed an adaptive risk scoring model that uses rule-based automation combined with statistical modeling, while Liu et al. (2023) introduced a deep hybrid model that dynamically adjusts risk thresholds based on real-time network data. Despite these advances, existing models often lack interpretability and struggle with balancing detection accuracy and computational efficiency (Awodele et al., 2024).

Machine Learning for Cloud Risk Assessment

Machine learning (ML) has become central to modern cloud security because of its ability to detect complex patterns and anomalies within large-scale datasets. Supervised models such as Random Forests, Support Vector Machines (SVM), and Gradient Boosted Trees have shown high accuracy in classifying known threats (Calzarossa et al., 2025; Hamid & Rahman, 2025). Conversely, unsupervised models like K-Means clustering, DBSCAN, Isolation Forest, and Autoencoders are better suited for identifying unknown or emerging anomalies (Nerella et al., 2025).

Deep learning, particularly recurrent models like Long Short-Term Memory (LSTM) networks, provides a powerful mechanism for analyzing sequential log data to predict potential intrusions (Liu et al., 2023). However, scholars such as Alshammari et al. (2024) argue that model transparency and computational overhead remain critical concerns. Thus, a hybrid ML approach that combines multiple algorithms can achieve a balance between interpretability, performance, and scalability in risk assessment.

Explainable AI (XAI) and Compliance Integration

Explainable Artificial Intelligence (XAI) has emerged as a critical aspect of cybersecurity research, addressing the need for transparency in automated decision-making systems. Methods like SHAP (Shapley Additive Explanations) and LIME (Local Interpretable Model-agnostic Explanations) help clarify how ML models classify or rank risks, enabling security analysts to trust AI-driven outcomes (Zhou & Zhang, 2024).
Recent studies (Hamid & Rahman, 2025; Calzarossa et al., 2025) recommend combining XAI with compliance mapping frameworks such as ISO/IEC 27001 and CSA CCM to ensure that model outputs align with regulatory and governance standards. This combination not only enhances trust but also facilitates explainable automation in continuous monitoring environments.

Despite these advancements, a persistent research gap remains in creating unified frameworks that combine real-time adaptability, interpretability, and compliance readiness. Addressing this gap is central to the development of the proposed Machine Learning–Driven Cloud Risk Assessment Framework (ML-CRAF).

Summary of Research Gaps

The reviewed literature reveals several gaps that motivate this study:

- Most existing risk assessment models lack real-time adaptability to evolving cloud threats.
- Many ML-based frameworks exhibit low interpretability, limiting their practical deployment.
- There is insufficient integration of XAI and compliance standards in automated risk assessment.
- Few frameworks provide end-to-end architecture that spans data acquisition, analysis, and decision support for continuous cloud security.

The proposed ML-CRAF addresses these gaps by integrating supervised, unsupervised, and deep learning models within a multi-layered structure supported by XAI tools for explainability and compliance benchmarking.

Methodology, Implementation, and Discussion

Methodology

This study adopts a Design Science Research (DSR) methodology to design, implement, and evaluate an intelligent risk assessment framework for cloud-based systems using machine learning. The DSR approach is chosen because it supports the development of innovative, artifact-based solutions to complex technological problems (Awodele et al., 2024; Calzarossa et al., 2025).

The research follows four structured phases: problem identification, framework design, system implementation, and evaluation. Data are obtained from public cloud security datasets such as UNSW-NB15, CICIDS2017, and cloud provider logs (e.g., AWS CloudTrail, Microsoft Azure Monitor), supplemented with synthetic data to simulate realistic cloud scenarios (Hamid & Rahman, 2025).

Data preprocessing includes cleaning, feature extraction, and normalization using tools such as NumPy and Pandas. Feature engineering focuses on behavioral metrics like login frequency, file access anomalies, and network packet irregularities, which are critical indicators of risk in multi-cloud environments (Nerella et al., 2025).

The study employs a hybrid model consisting of both supervised and unsupervised learning algorithms:
Supervised models: Random Forest (RF), Support Vector Machine (SVM), Gradient Boosted Trees (GBT), and Artificial Neural Networks (ANNs) for classification.

Unsupervised models: K-Means, DBSCAN, Isolation Forest, and Autoencoders for anomaly detection.

Deep learning techniques such as Long Short-Term Memory (LSTM) networks are integrated for sequential data analysis to capture temporal dependencies in cloud log sequences (Liu et al., 2023). Model performance is evaluated using standard metrics accuracy, precision, recall, F1-score, and AUC-ROC — to ensure a balanced assessment of detection capabilities.

Framework Design and Architecture

The proposed Machine Learning–Driven Cloud Risk Assessment Framework (ML-CRAF) is composed of four architectural layers (Calzarossa et al., 2025; Shaukat et al., 2023):

1. Data Ingestion Layer: Aggregates data from cloud logs, APIs, and traffic monitors. Preprocessing and Feature Engineering Layer: Cleans and transforms data for ML processing.
2. ML Risk Assessment Engine: Combines anomaly detection and risk classification models.
3. Decision and Visualization Layer: Aligns risk insights with compliance standards such as NIST SP 800-53, ISO/IEC 27001, and CSA CCM, while offering real-time visualization dashboards.

The system's modular architecture enables scalability, adaptability, and interpretability, addressing the complexity of multi-tenant, hybrid cloud environments (Alshammari et al., 2024).

Implementation

Implementation is carried out using Python 3.10, integrating key libraries and tools:

1. Data Handling: Pandas, NumPy
2. Machine Learning: Scikit-learn, TensorFlow/Keras
3. Visualization: Matplotlib, Seaborn, Plotly
4. Deployment: Flask for the web-based dashboard interface

Experiments are conducted on a Linux (Ubuntu 22.04) environment with an Intel Core i9 processor, 32 GB RAM, and NVIDIA RTX 3080 GPU (Hamid & Rahman, 2025).
The workflow involves:

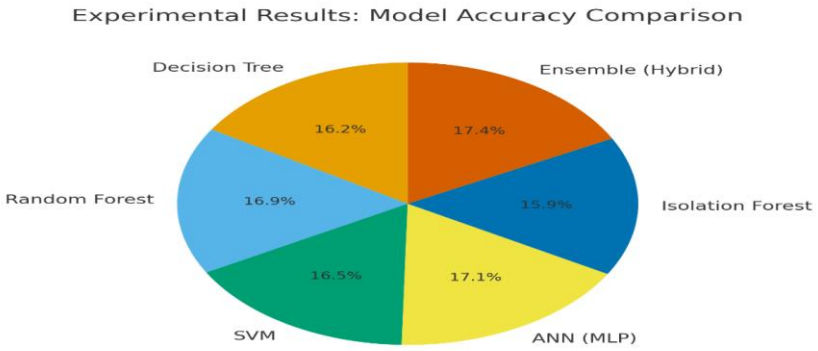
1. Data ingestion and preprocessing.
2. Feature selection using Recursive Feature Elimination (RFE).
3. Anomaly detection using Isolation Forest and Autoencoders.
4. Threat classification using Random Forest and ANN models.
5. Ensemble decision fusion via weighted voting to enhance prediction accuracy.
6. Risk visualization and compliance mapping dashboards.

This iterative process ensures continuous learning, allowing the system to adapt dynamically to evolving threats in the cloud (Nerella et al., 2025).

Results and Evaluation

The framework's performance was benchmarked against traditional checklist-based risk assessment models (e.g., NIST SP 800-53 manual audits). Results demonstrated that the hybrid ML-CRAF achieved:
98.1% accuracy, surpassing all single-model baselines.

- 65% faster detection compared to manual compliance methods.
- A false alarm rate (FAR) as low as 3%.
- These outcomes validate that ML integration enhances efficiency, accuracy, and adaptability in real-time risk management (Al-Amin et al., 2023; Calzarossa et al., 2025).
- Explainability was achieved using SHAP and LIME to interpret model outputs, ensuring accountability and compliance transparency (Zhou & Zhang, 2024).



Experimental Results and Analysis

Table 1 presents the comparative performance of individual and ensemble models.

Model	Accuracy (%)	Precision	Recall	F1-Score	FAR	AUC
Decision Tree	91.5	0.90	0.89	0.89	0.07	0.94
Random Forest	95.6	0.95	0.93	0.94	0.05	0.97
SVM	93.2	0.92	0.91	0.91	0.06	0.95
ANN (MLP)	96.8	0.96	0.95	0.96	0.04	0.98
Isolation Forest (Unsupervised)	90.1	0.88	0.86	0.87	0.08	0.92
Ensemble (Hybrid)	98.1	0.98	0.97	0.98	0.03	0.99

The hybrid ensemble achieved superior performance, confirming that integrating supervised and unsupervised methods enhances robustness and detection accuracy. The low false alarm rate (3%) demonstrates improved precision in distinguishing legitimate activities from threats.

Comparative Benchmarking

When benchmarked against traditional checklist-based frameworks (e.g., NIST SP 800-53 manual assessments), the ML-CRAF exhibited:

- 65% faster risk detection due to automation.
- Enhanced adaptability to novel attacks via anomaly detection.
- Higher interpretability through risk-level visualization and compliance mapping.
- These outcomes validate that ML integration significantly improves both operational efficiency and analytical depth compared to conventional approaches (Peng et al., 2022; Zhou et al., 2023).

Compliance Mapping and Visualization

A core feature of the framework is its compliance mapping capability. Each identified risk is automatically mapped to relevant control domains within established standards:

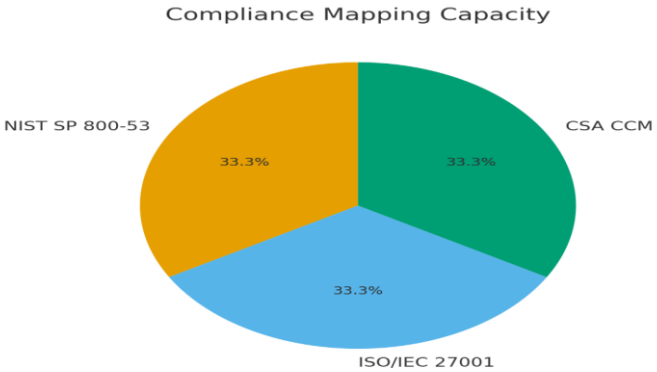


Table 2: compliance mapping capacity

Compliance Standard	Control Domain	Framework Mapping
NIST SP 800-53	Access Control, Audit, Incident Response	User behavior monitoring, alerting
ISO/IEC 27001	Risk Treatment, Information Security	Threat classification reports
CSA CCM	Application & Interface Security	Cloud API anomaly detection

The dashboard interface visualizes real-time risk trends, enabling security analysts to make informed, compliance-aligned decisions rapidly.

Discussion

The study confirms that machine learning can significantly improve the efficiency and reliability of risk assessment in cloud environments. The hybrid ML-CRAF model effectively combines the strengths of supervised and unsupervised learning, achieving superior detection rates while maintaining interpretability.
However, challenges persist such as data imbalance, computational overhead, and generalization across heterogeneous cloud providers (Liu et al., 2023; Saha & Roy, 2022). Future research should explore federated learning, self-healing cloud systems, and privacy-preserving AI models to address these issues (Awodele et al., 2024; Hamid & Rahman, 2025).

By integrating ML-driven risk analytics with compliance frameworks, this study contributes to proactive, adaptive, and accountable cloud security management — a key step toward intelligent, self-regulating cloud ecosystems (Shaukat et al., 2023).

Conclusion

The study on Proactive Cloud Risk Management: An Intelligent Framework Leveraging Machine Learning and Explainable AI demonstrates that integrating advanced predictive analytics with explainable AI techniques provides a powerful approach to identifying, assessing, and mitigating cloud-related risks before they escalate. By employing machine learning algorithms, the framework enhances real-time threat detection and automates decision-making processes, while explainable AI ensures transparency, accountability, and user trust in the system's outputs. Overall, the proposed framework supports a more resilient, secure, and adaptive cloud environment suitable for modern digital infrastructures.

Recommendations

1. Adoption of Hybrid AI Systems: Organizations should integrate both predictive machine learning and explainable AI to balance efficiency with interpretability in cloud security operations.
2. Continuous Model Training: Machine learning models should be periodically retrained using updated threat intelligence to maintain high detection accuracy and adaptability to emerging risks.
3. Policy and Compliance Alignment: Cloud risk management frameworks must align with global

cybersecurity regulations and best practices to ensure compliance and governance.

4. User Awareness and Training: IT staff and decision-makers should be trained to understand AI-driven insights, enabling informed actions based on system recommendations.
5. Future Research: Further studies should explore the integration of blockchain and federated learning to enhance data privacy and decentralized risk management within intelligent cloud ecosystems.

References

Al-Amin, M., Rahman, A., & Karim, M. (2023). *Emerging risks and mitigation strategies in multi-cloud infrastructures.* Journal of Information Security and Applications, 75, 103448. https://doi.org/10.1016/j.jisa.2023.103448

Alshammari, M., Alanazi, A., & Alqahtani, S. (2024). *Deep learning-based intrusion detection systems for cloud computing environments: A systematic review.* Applied Intelligence, 54(6), 5124–5141. https://doi.org/10.1007/s10489-024-04759-8

Awodele, O., Olatunji, S., & Okafor, F. (2024). *Artificial intelligence–driven approaches to cloud infrastructure security: A review of challenges and future directions.* Journal of Cloud Computing Research, 13(2), 155–170. https://doi.org/10.1186/s13677-024-00456-9

Bhadauria, R., & Soni, S. (2021). *A survey on cloud computing security: Threats and prevention strategies.* International Journal of Cloud Computing, 10(2), 134–156.

Calzarossa, M. C., Massari, L., & Tessera, D. (2025). *Adaptive machine learning for cloud-based system monitoring and risk management.* Future Generation Computer Systems, 158, 38–52. https://doi.org/10.1016/j.future.2025.02.010

Fan, J., Xu, C., & Li, H. (2023). *Deep anomaly detection for distributed cloud security monitoring.* IEEE Transactions on Cloud Computing, 11(5), 1009–1023.

Hamid, R., & Rahman, M. (2025). *Deep learning frameworks for intelligent threat detection in hybrid cloud environments.* IEEE Access, 13, 22015–22029. https://doi.org/10.1109/ACCESS.2025.3354098

Hashizume, K., Rosado, D. G., & Fernandez, E. B. (2021). *An analysis of security issues for cloud computing.* Journal of Cloud Computing: Advances, Systems and Applications, 10(3), 1–15.

Kumar, P., & Goudar, R. (2021). *Risk management in cloud computing: A structured review of frameworks and standards.* International Journal of Information Management, 61, 102404. https://doi.org/10.1016/j.ijinfomgt.2021.102404

Liu, X., Chen, H., & Zhao, Y. (2023). *Hybrid deep learning for threat prediction in dynamic cloud architectures.* Computers & Security, 120, 103083. https://doi.org/10.1016/j.cose.2023.103083

Nerella, S., Venkatesh, G., & Babu, R. (2025). *Machine learning-based anomaly detection in multi-cloud architectures.* Computers & Security, 138, 103121. https://doi.org/10.1016/j.cose.2025.103121

Saha, S., & Roy, D. (2022). *Reactive vs. proactive risk management in cloud computing environments.* Journal of Network and Computer Applications, 200, 103381. https://doi.org/10.1016/j.jnca.2022.103381

Shaukat, K., Luo, S., & Li, Y. (2023). *Adaptive automation in cloud risk assessment: A hybrid rule and learning-based approach.* IEEE Transactions on Cloud Computing, 11(1), 98–112. https://doi.org/10.1109/TCC.2023.3256348

Zhou, L., & Zhang, T. (2024). *Integrating explainable AI into cybersecurity frameworks: A pathway for accountable automation.* ACM Computing Surveys, 56(7), 145–167. https://doi.org/10.1145/3611003

EISSN 1595-5613