AI Power-Driven Threat Detection and Behaviour Risk Scroling System in Cloud Environments

H.S. Arusree[1], Dr. N. Sathyabalaji[2], M.C. Savithri[3], L. Dharani[4]
[1,2,3,4]*Department of Computer Science and Engineering, J.K.K. Munirajah College of Technology, Erode, Tamil Nadu, India.*

***Abstract*—Cloud computing continues to evolve with the integration of cutting-edge technologies such as Zero Trust Architecture (ZTA), Confidential Computing, Artificial Intelligence (AI), Blockchain, and Quantum-Resistant Cryptography. These advancements introduce new opportunities and challenges in managing sensitive user data. This paper presents an enhanced framework that integrates modern technologies into measurable, safe, and secure cloud data management. The proposed system leverages AI-driven anomaly detection, blockchain-based immutable auditing, homomorphic encryption, and confidential computing environments to ensure real-time verification, data integrity, and regulatory compliance. The framework introduces dynamic trust scoring and continuous monitoring to eliminate reliance on static security assumptions. Experimental evaluation demonstrates improved resilience, transparency, and scalability with acceptable performance overhead. This approach enables sensitive users to transition from trust-based systems to verifiable and measurable cloud security ecosystems.**

***Index Terms*—Cloud Security, Zero Trust, Confidential Computing, Blockchain, AI Security, Data Privacy, Quantum Cryptography.**

I. INTRODUCTION

Cloud computing has rapidly transformed the way organizations store, process, and manage data, offering scalability, flexibility, and cost-efficiency. However, as cloud adoption increases, so do concerns regarding data security, privacy, and trust. Traditional security models, which rely heavily on perimeter-based defenses and implicit trust, are no longer sufficient in the face of sophisticated cyber threats and evolving regulatory requirements. To address these challenges, modern cloud security paradigms are shifting toward integrated, technology-driven approaches that emphasize verification, transparency, and resilience. This paper proposes an enhanced cloud data management framework that incorporates advanced technologies such as Zero Trust Architecture (ZTA), Confidential Computing, Artificial Intelligence (AI), Blockchain, and Quantum-Resistant Cryptography.

Zero Trust Architecture represents a fundamental shift from conventional trust models by enforcing the principle of "never trust, always verify." In this approach, every access request whether originating inside or outside the network is continuously authenticated, authorized, and validated. By eliminating implicit trust, ZTA minimizes the attack surface and reduces the risk of lateral movement within cloud environments. The proposed framework extends ZTA by introducing dynamic trust scoring, which evaluates user and system behavior in real time. This scoring mechanism adapts based on contextual factors such as access patterns, device integrity, and historical behavior, enabling more granular and adaptive access control decisions.

Confidential Computing further enhances data security by protecting sensitive information during processing, not just at rest or in transit. Using hardware-based Trusted Execution Environments (TEEs), confidential computing ensures that data remains encrypted even while being processed, preventing unauthorized access from privileged insiders or compromised system components. In the proposed framework, confidential computing is integrated with homomorphic encryption techniques, allowing computations to be performed on encrypted data without requiring decryption. This combination significantly reduces exposure risks while enabling secure data analytics and processing in untrusted cloud environments.

Artificial Intelligence plays a crucial role in strengthening cloud security through intelligent monitoring and threat detection. The framework incorporates AI-driven anomaly detection systems that continuously analyze network traffic, user behavior, and system activities to identify deviations from normal patterns. Unlike traditional rule-based systems, AI models can adapt to evolving threats and detect previously unknown attack vectors. Machine learning algorithms are trained on large datasets to recognize subtle indicators of compromise, enabling early detection and rapid response. This proactive approach enhances the overall resilience of the cloud infrastructure and reduces the likelihood of successful attacks.

Blockchain technology is utilized within the framework to ɯɥɯhnɥ data integrity, transparency, and accountability. By maintaining an immutable and decentralized ledger of all transactions and access events, blockchain ensures that records cannot be altered or tampered with. This feature is particularly valuable for auditing and compliance purposes, as it provides verifiable proof of data access and modifications. Smart contracts can be employed to automate policy enforcement and compliance checks, reducing the need for manual intervention and minimizing human error. The integration of blockchain-based auditing mechanisms enhances trust among stakeholders and supports regulatory requirements for data governance.

Another critical component of the proposed framework is Quantum-Resistant Cryptography, which addresses the emerging threat posed by quantum computing. As quantum technologies advance, traditional cryptographic algorithms such as RSA and ECC may become vulnerable to attacks. To ensure long-term data protection, the framework incorporates post-quantum cryptographic algorithms that are designed to withstand quantum attacks. This forward-looking approach ensures that sensitive data remains secure even in the face of future technological advancements.

The framework also emphasizes continuous monitoring and real-time verification, replacing static security assumptions with dynamic, evidence-based decision-making. By integrating data from multiple sources including AI analytics, blockchain logs, and trust scores the system provides a comprehensive and up-to-date view of the security posture. Automated response mechanisms can be triggered when anomalies or policy violations are detected, enabling rapid containment and mitigation of threats.

Experimental evaluation of the proposed framework demonstrates significant improvements in key performance metrics, including security resilience, transparency, and scalability. While the integration of advanced technologies introduces some performance overhead, the results indicate that this overhead remains within acceptable limits for most practical applications. The benefits of enhanced security and trust far outweigh the additional computational costs, particularly for organizations handling sensitive or regulated data.

In conclusion, the evolving landscape of cloud computing demands innovative approaches to data security and management. The integration of Zero Trust Architecture, Confidential Computing, Artificial Intelligence, Blockchain, and Quantum-Resistant Cryptography provides a comprehensive and future-proof solution for securing cloud environments. By shifting from trust-based models to verifiable and measurable security mechanisms, the proposed framework enables organizations to confidently manage sensitive data in the cloud. This approach not only addresses current security challenges but also prepares for emerging threats, ensuring a robust and sustainable cloud security ecosystem.

II. PROCEDURE FOR PAPER SUBMISSION

2.1. Cloud Computing infrastructure

Cloud security has been an active area of research due to the rapid adoption of cloud infrastructures and the increasing volume of sensitive data stored and processed in distributed environments. Existing literature highlights several key approaches, including Zero Trust Architecture (ZTA), blockchain-based trust systems, confidential computing, artificial intelligence-driven security, and advanced cryptographic techniques. This section reviews major contributions in these domains and identifies research gaps that motivate the proposed framework.

Early studies on cloud security primarily focused on traditional mechanisms such as encryption, access control, and intrusion detection systems. However, as cloud environments became more complex and dynamic, these approaches were found insufficient to address modern threats. A comprehensive survey on

cloud, edge, and fog computing security emphasizes that the growing attack surface, multi-tenancy, and distributed architecture introduce significant vulnerabilities, requiring more adaptive and integrated security models. Similarly, recent work highlights that despite widespread adoption, ensuring data confidentiality, integrity, and availability remains a major challenge in cloud systems, particularly in sectors such as finance and government.

One of the most significant advancements in recent years is the adoption of Zero Trust Architecture. Unlike traditional perimeter-based security models, ZTA assumes that no entity should be trusted by default. Research by Sarkar et al. presents a comparative review of zero-trust models, noting that ZTA enforces continuous authentication and behavior-based trust evaluation to enhance security in cloud networks. Further studies indicate that ZTA incorporates principles such as least privilege access, micro-segmentation, and continuous monitoring, significantly reducing the risk of insider threats and lateral attacks. However, existing implementations face challenges related to scalability, performance overhead, and integration with legacy systems, indicating the need for more efficient and adaptive frameworks.

Blockchain technology has also emerged as a promising solution for improving trust and transparency in cloud computing. Several studies propose blockchain-based trust management systems that utilize decentralized ledgers to record transactions and access events immutably. A taxonomy of blockchain-based approaches highlights their effectiveness in addressing trust issues, ensuring data integrity, and enabling secure data sharing among multiple stakeholders. Additionally, systematic literature reviews show that blockchain can enhance authentication, auditing, and service-level agreement enforcement in cloud environments. Despite these advantages, challenges such as scalability, latency, and energy consumption limit the practical deployment of blockchain in large-scale cloud systems.

Confidential computing has gained attention as a solution to protect data during processing, addressing the “data-in-use” security gap. Traditional encryption methods secure data at rest and in transit but fail to protect it during computation. Recent surveys on confidential computing highlight the use of Trusted Execution Environments (TEEs) to ensure secure data processing even in untrusted environments. Research also explores the integration of confidential computing with machine learning, enabling secure model training and inference on sensitive data. However, limitations such as hardware dependency, performance overhead, and potential vulnerabilities in enclave technologies remain open research challenges.

2.2. Quantum-resistant cryptography

Artificial Intelligence and Machine Learning have been widely applied to enhance cloud security through intelligent threat detection and automated response mechanisms. AI-driven systems analyze large volumes of data to identify anomalies, detect intrusions, and predict potential attacks. Recent studies propose integrating AI with cloud security frameworks to enable adaptive policy enforcement and real-time monitoring. While AI significantly improves detection accuracy and response time, it also introduces new challenges, including model bias, adversarial attacks, and increased system complexity.

Another emerging area of research is quantum-resistant cryptography, which addresses the potential threat posed by quantum computing to classical encryption algorithms. Although still in its early stages, post-quantum cryptographic techniques are being developed to ensure long-term data security. Existing literature suggests that integrating quantum-resistant algorithms into cloud systems is essential for future-proofing security infrastructures, particularly for sensitive and long-lived data.

Several recent studies attempt to combine multiple technologies to create comprehensive cloud security frameworks. For example, hybrid models integrating Zero Trust, blockchain, and AI-driven policies have been proposed to enhance security, scalability, and automation in cloud environments. These approaches demonstrate the effectiveness of combining complementary technologies; however, most existing frameworks lack unified mechanisms for real-time verification, dynamic trust evaluation, and measurable security metrics.

2.3. Synthesis and Identified Gap

In summary, the literature indicates that while significant progress has been made in individual areas such as Zero Trust, blockchain, confidential computing, and AI-based security, there is still a lack

of fully integrated frameworks that combine these technologies into a cohesive and scalable solution. Existing approaches often address specific aspects of cloud security but fail to provide end-to-end protection, continuous trust evaluation, and verifiable security guarantees. Furthermore, challenges related to performance overhead, interoperability, and regulatory compliance remain unresolved.

III. PROPOSED FRAMEWORK AND METHODOLOGY

The proposed framework presents a unified and secure cloud data management architecture that integrates Zero Trust principles, Artificial Intelligence (AI), Blockchain, Confidential Computing, and Quantum-Resistant Cryptography. The primary objective is to move from static, trust-based systems to a dynamic, verifiable, and measurable security ecosystem. This section describes the architecture, core components, and methodology adopted for implementation and evaluation.

The architecture is designed as a multi-layered model consisting of five key players: (i) User Access Layer, (ii) Trust Evaluation Layer, (iii) Secure Processing Layer, (iv) Data Integrity and Audit Layer, and (v) Cryptographic Protection Layer. Each layer contributes to enforcing continuous verification, secure computation, and transparent auditing.

At the core of the framework is the Zero Trust principle, where no user, device, or application is trusted by default. Every access request undergoes continuous authentication, authorization, and validation. The system integrates AI-driven analytics, blockchain-based logging, and confidential computing environments to ensure end-to-end security.

3.1 Zero Trust Access Control

This module enforces strict identity verification and least-privilege access. Multi-factor authentication (MFA), device validation, and micro-segmentation are implemented to restrict unauthorized access. Unlike traditional models, access decisions are not static but continuously updated based on user behavior and system context.

3.2 Dyunamic Trust Scoring Systemero Control

A novel contribution of the framework is the dynamic trust scoring mechanism. Each user and device is assigned a trust score based on multiple parameters, including login patterns, geolocation, device health, and historical activity. The trust score is continuously updated using AI models. Access privileges are adjusted dynamically—higher trust scores allow smoother access, while lower scores trigger additional verification or denial.

3.3. AI-Based Anomaly Detection

The framework employs machine learning algorithms to monitor network traffic, user behavior, and system logs in real time. Supervised and unsupervised learning models are used to detect anomalies such as unusual login attempts, data exfiltration patterns, and insider threats. The AI engine improves over time through continuous learning, enabling early detection of previously unknown attacks.

3.4. Blockchain-Based Audit and Integrity Module

All transactions, access logs, and policy changes are recorded on a blockchain ledger. This ensures immutability, transparency, and traceability of all operations. Smart contracts are used to enforce security policies automatically, ensuring compliance with regulatory standards. The decentralized nature of blockchain eliminates single points of failure and enhances trust among stakeholders.

3.5. Quantum-Resistant Cryptographic blockchain

To address future threats posed by quantum computing, the framework incorporates post-quantum cryptographic algorithms. These algorithms replace or complement traditional encryption techniques, ensuring long-term data protection. This layer secures data at rest, in transit, and during key exchange processes.

IV. EVALUATION: RESULTS AND DISCUSSION

To rigorously evaluate the effectiveness of the proposed AI-Powered Insider Threat Detection and Behavior Risk Scoring System, a comprehensive experimental study was conducted within a controlled yet realistic cloud computing environment. The evaluation aimed to simulate enterprise-level operations where multiple users interact with shared resources, applications, and sensitive data. This setup enabled the system to be tested under conditions that closely resemble real-world scenarios involving insider threats.

The dataset used in this study was composed of detailed user activity logs collected from various simulated sources, including authentication systems, file servers, database access logs, and network monitoring tools. These logs captured a wide range of behavioral attributes such as login frequency, session duration, file access patterns, command execution sequences, data transfer volumes, and access to privileged resources. To ensure robustness, the dataset incorporated both benign user behavior and multiple categories of insider threat activities. These included malicious actions such as unauthorized data access, privilege escalation, data exfiltration, and abnormal login behavior (e.g., logins from unusual locations or times).

Data preprocessing played a critical role in preparing the dataset for analysis. Raw logs were first cleaned to remove inconsistencies, duplicates, and missing values. Feature engineering techniques were then applied to extract meaningful behavioral indicators. For example, features such as "average login interval," "file access deviation score," and "resource usage anomaly index" were derived to quantify user behavior more effectively. The dataset was normalized to ensure consistency across features and prevent bias during model training.

The dataset was divided into training and testing subsets using a standard split ratio (e.g., 70:30), ensuring that the model was evaluated on unseen data. Multiple Machine Learning (ML) models were implemented to analyze user behavior. These included supervised learning algorithms such as Decision Trees, Random Forests, and Support Vector Machines (SVM), as well as unsupervised anomaly detection techniques like Isolation Forest and K-Means clustering. The combination of supervised and unsupervised approaches allowed the system to detect both known and unknown threat patterns.

A key component of the proposed system is the dynamic risk scoring mechanism. Each user is assigned a risk score based on deviations from their established behavioral baseline. This score is continuously updated as new data is processed, enabling real-time monitoring and early detection of suspicious activities. The system architecture supports continuous data ingestion and real-time analysis, making it suitable for modern cloud environments.

The evaluation results demonstrate that the proposed system achieves high detection accuracy, improved recall, and reduced false positive rates compared to traditional methods. The integration of real-time monitoring and adaptive learning ensures that the system remains effective even in complex and large-scale cloud environments. Additionally, the system's scalability makes it suitable for deployment in organizations with a large number of users and high data volumes.

The system focuses on understanding user behavior by analyzing activity patterns such as login behavior, file access, and resource utilization. By establishing a baseline for normal user activity, it becomes possible to detect anomalies that may indicate malicious intent. One of the key strengths of the proposed approach is its ability to continuously learn and adapt to changing user behavior, making it more effective in identifying previously unknown threats.

V. CONCLUSION

In this work, an AI-Powered Insider Threat Detection and Behavior Risk Scoring System was proposed to address the growing challenges of securing cloud computing environments against insider threats. Traditional security systems, which rely on static rules and predefined signatures, are often inadequate in detecting sophisticated and evolving threats originating from within an organization. To overcome these limitations, the proposed system adopts a dynamic and intelligent approach by leveraging Machine Learning (ML) and behavioral analytics. A significant contribution of this system is the implementation of a dynamic risk scoring mechanism. Each user is assigned a risk score based on deviations from their normal behavior, allowing security administrators to identify high-risk users in real time. This proactive approach enhances the overall security posture by enabling early detection and timely intervention, thereby reducing the potential impact of insider attacks. However, certain limitations were identified. The performance of the system depends on the availability of high-quality training data, and real-time processing may require significant computational resources. Privacy concerns related to user monitoring must also be addressed through appropriate safeguards and compliance with data protection regulations.

Overall, the proposed system represents a significant advancement in insider threat detection by combining

intelligence, adaptability, and real-time analysis into a unified framework.

REFERENCES

[1] B. Bin Sarhan and N. Altwaijry, "Insider threat detection using machine learning approach," *Applied Sciences*, vol. 13, no. 1, 2023, doi: 10.3390/app13010259.

[2] M. N. Al-Mhiqani *et al*., "A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges," *Applied Sciences*, vol. 10, no. 15, 2020.

[3] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Computers & Security*, 2021.

[4] Al-Shehari *et al*., "Insider threat detection model using isolation forest," *IEEE Access*, 2023.

[5] Z. Tian *et al*., "Deep learning and Dempster–Shafer theory-based insider threat detection," *Mobile Networks and Applications*, 2020.

[6] M. Haq *et al*., "Insider threat detection based on NLP word embedding and ML," *Intelligent Automation & Soft Computing*, 2022.

[7] M. Al-Saedi *et al*., "A new intelligent multilayer framework for insider threat detection," *Computers & Electrical Engineering*, 2022.

[8] Ali *et al*., "Real-time detection of insider threats using behavioral analytics," 2025.

[9] X. Liu *et al*., "Handling imbalanced dataset in insider threat detection," *Computers & Electrical Engineering*, 2024.

[10] J. Brown *et al*., "Insider threat detection: Lessons from real deployment," *Journal of Information Security and Applications*, 2022.