International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

ADAPTIVE CLOUD SECURITY USING ML-DRIVEN AUTHENTICATION AND CRYPTO-AGILE ENCRYPTION

[1] Darzi Mehtaab Siddiqa, [2] Myle Vijayalakshmi, [3] Kuruva Sravani, [4] Mala Anitha, [5] Kyrupla Harika
[1] *Assistant Professor,* [2345] *Students*
Department of Computer Science and Engineering
St. Johns College Of Engineering & Technology, Yerrakota, Yemmiganur, Kurnool, A.P.
mehtaabd2001@gmail.com, vijayalakshmimyle264@gmail.com, sravanikuruva082@gmail.com, malaanitha2004@gmail.com, harikakyrupla@gmail.com

ABSTRACT

Cloud computing has become a critical component of modern digital infrastructure; however, traditional authentication mechanisms and static cryptographic configurations remain vulnerable to evolving cyber threats. This paper presents an intelligent and adaptive cloud security framework that integrates machine learning–driven multi-factor authentication (MFA) with dynamic cryptographic agility. The proposed system employs behavioral analytics, contextual risk assessment, and continuous monitoring to classify authentication requests in real time. A hybrid deep learning model is utilized to predict potential attack patterns and assign dynamic risk scores, enabling adaptive enforcement of authentication factors.

Unlike conventional static security architectures, the framework incorporates adaptive cryptography that dynamically selects encryption algorithms and key parameters based on assessed threat levels and data sensitivity. This ensures strong protection for high-risk sessions while maintaining performance efficiency for low-risk interactions. The integration of anomaly detection, continuous authentication, and crypto-agile mechanisms significantly enhances resistance against credential stuffing, replay attacks, session hijacking, and impersonation attempts.

Experimental evaluation demonstrates improved authentication accuracy, reduced false acceptance rates, optimized encryption overhead, and scalable performance under high-load cloud environments. The results confirm that combining machine learning intelligence with adaptive multi-layer cryptographic protection establishes a resilient, future-ready cloud security architecture.

Keywords: Cloud Security, Multi-Factor Authentication (MFA), Machine Learning, Adaptive Cryptography, Crypto Agility, Risk-Based Authentication, Behavioral Biometrics, Intrusion Detection System (IDS), Continuous Authentication, Post-Quantum Readiness..

I. INTRODUCTION

Cloud computing has transformed modern computing by enabling scalable, on-demand, and distributed access to storage, processing power, and applications. Organizations increasingly rely on cloud platforms to manage critical data, enterprise applications, and financial transactions. However, this rapid adoption has significantly expanded the attack surface, exposing cloud infrastructures to sophisticated cyber threats. Traditional perimeter-based security and static authentication mechanisms are no longer sufficient to protect sensitive cloud environments.

Conventional authentication systems predominantly rely on password-based or basic multi-factor mechanisms that operate using fixed rules. These static approaches fail to adapt to contextual variations, behavioral changes, or emerging attack strategies. As attackers leverage credential stuffing, phishing, replay attacks, and session hijacking, there is a growing need for intelligent, adaptive, and risk-aware security frameworks.

Machine learning has emerged as a powerful tool for enhancing authentication systems by enabling behavioral analysis, anomaly detection, and predictive threat modeling. By analyzing historical login patterns, device attributes, geolocation, and session activity, ML models can distinguish legitimate users from malicious actors with higher accuracy. When combined with adaptive multi-factor authentication (MFA) and dynamic cryptographic selection, such systems provide a proactive and resilient defense mechanism.

This work proposes an intelligent cloud security architecture that integrates machine learning–driven risk-based authentication with adaptive cryptographic agility. The framework continuously evaluates user trust levels and dynamically adjusts authentication requirements and

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

encryption strength according to assessed risk. By unifying authentication intelligence, intrusion detection, and crypto-agile mechanisms, the proposed system enhances cloud security while maintaining usability and scalability.

OBJECTIVES

The primary objectives of the proposed system are as follows:

1. To design an adaptive multi-factor authentication framework that integrates knowledge-based, contextual, and behavioral factors to strengthen cloud access control.
2. To implement machine learning–based risk assessment models capable of detecting anomalous login behavior and predicting potential attack patterns in real time.
3. To develop a continuous authentication mechanism that monitors user activity throughout active sessions to prevent session hijacking and insider threats.
4. To incorporate adaptive cryptography and cryptographic agility, enabling dynamic selection of encryption algorithms and key parameters based on risk level and data sensitivity.
5. To reduce false acceptance and false rejection rates by leveraging behavioral analytics and intelligent decision-making models.
6. To enhance system scalability and performance while maintaining strong security in high-load cloud environments.
7. To provide a unified security framework that integrates authentication, intrusion detection, and encryption into a coordinated cloud defense architecture.

II. LITERATURE SURVEY

Cloud computing security has evolved significantly over the past decade due to increasing cyber threats targeting authentication systems, credential storage, and cloud-hosted data. Researchers have focused on strengthening authentication frameworks, enhancing cryptographic mechanisms, and integrating intelligent threat detection systems to improve cloud security resilience.

1. Evolution of Cloud Authentication Mechanisms

Early cloud authentication systems primarily relied on single-factor authentication using static passwords. Studies revealed that password-based mechanisms are highly vulnerable to phishing, brute-force attacks, credential stuffing, and replay attacks. To mitigate these risks, researchers introduced Multi-Factor Authentication (MFA), combining knowledge-based, possession-based, and inherence-based factors.

Although MFA significantly reduces unauthorized access, traditional MFA implementations remain static and apply identical verification procedures regardless of contextual risk. Recent research highlights the need for adaptive MFA frameworks that dynamically adjust authentication requirements based on device trust, geolocation, behavioral consistency, and risk indicators.

2. Machine Learning in Authentication Systems

Machine Learning (ML) has emerged as a transformative approach for enhancing authentication security. Unlike rule-based systems, ML models can analyze large volumes of behavioral and contextual data to identify subtle anomalies.

Behavioral biometrics such as keystroke dynamics, mouse movement patterns, and device interaction behaviors are increasingly used for continuous authentication. Supervised learning models classify authentication attempts as legitimate or malicious, while unsupervised anomaly detection techniques identify deviations from established user profiles.

Recent studies demonstrate that hybrid deep learning architectures, including Convolutional Neural Networks (CNNs) and Transformer-based models, improve classification accuracy in intrusion detection and behavioral analysis tasks. These approaches reduce both false acceptance rate (FAR) and false rejection rate (FRR), improving overall system reliability.

3. Risk-Based and Continuous Authentication

Risk-based authentication models assign dynamic risk scores to login attempts using contextual signals such as device fingerprinting, IP reputation, time-of-access anomalies, and historical login behavior. High-risk attempts trigger additional verification layers, while low-risk attempts are processed seamlessly to maintain usability.

Continuous authentication extends this concept beyond the initial login stage. Instead of verifying users only once, the system continuously evaluates session behavior. Research indicates that continuous verification significantly reduces the success rate of session

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

hijacking and insider attacks, which often bypass traditional login-based controls.

4. Cryptographic Protection and Template Security

Traditional cryptographic systems in cloud environments rely on fixed encryption algorithms and static key management strategies. However, static cryptography is increasingly vulnerable to evolving threats and emerging vulnerabilities.

To address these challenges, researchers propose hybrid cryptographic schemes that combine symmetric encryption, hashing algorithms, and key derivation functions to provide layered protection. Advanced studies explore lattice-based and post-quantum cryptographic mechanisms, such as ring-LWE, to secure biometric templates and protect against quantum-enabled attacks.

Biometric template protection remains a critical research area because biometric identifiers cannot be revoked if compromised. Transforming biometric data into secure cryptographic representations has been shown to enhance privacy and reduce template inversion risks.

5. Cryptographic Agility and Adaptive Encryption

Cryptographic agility refers to the ability of a system to transition between encryption algorithms and parameters without disrupting operations. As new vulnerabilities are discovered and post-quantum standards emerge, systems must adapt quickly.

Adaptive encryption frameworks dynamically adjust encryption strength based on risk level and data sensitivity. High-risk sessions may invoke stronger encryption algorithms and larger key sizes, while low-risk operations use lightweight cryptographic mechanisms to maintain performance efficiency. Research confirms that crypto-agile architectures enhance long-term resilience without significantly increasing computational overhead.

6. Integration of Intrusion Detection with Authentication

Traditional intrusion detection systems (IDS) operate independently from authentication modules, limiting coordinated threat response. Recent research integrates ML-based IDS with authentication engines, enabling dynamic security decisions based on real-time threat intelligence.

Hybrid IDS models combining deep learning and statistical anomaly detection have shown improved detection of credential stuffing, replay attacks, and distributed intrusion attempts. This integrated approach supports proactive security enforcement rather than reactive mitigation.

III. SYSTEM ANALYSIS

Existing System

Existing cloud security systems primarily rely on traditional authentication mechanisms combined with static cryptographic configurations. Most cloud platforms implement password-based authentication or basic multi-factor authentication (MFA) using OTPs or hardware tokens. These systems operate on predefined rules and perform authentication mainly at the login stage without continuous monitoring.

Authentication decisions in existing systems are typically rule-based rather than intelligence-driven. Once access is granted, minimal behavioral analysis or session re-evaluation is performed. Cryptographic algorithms and key management policies are usually fixed during system deployment and rarely updated dynamically based on threat conditions.

Although some modern systems incorporate intrusion detection modules, these are often loosely integrated and operate independently of authentication workflows. As a result, authentication, encryption, and threat detection function as isolated components rather than as a unified security framework.

Disadvantages of Existing System

1. **Static Authentication Mechanism**
   Authentication workflows are fixed and do not adapt based on contextual risk, behavioral anomalies, or evolving threat patterns.
2. **Over-Reliance on Password-Based Security**
   Heavy dependence on passwords makes systems vulnerable to phishing, brute-force attacks, credential stuffing, and password reuse.
3. **Lack of Continuous Authentication**
   User identity is verified only at login, allowing attackers to exploit compromised sessions without further detection.
4. **Rigid Cryptographic Infrastructure**
   Encryption algorithms and key management strategies remain static, limiting responsiveness to emerging vulnerabilities or post-quantum threats.

ISSN 2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

5. **Limited Integration with Intelligent Threat Detection**
   Intrusion detection systems operate separately from authentication modules, preventing coordinated and real-time adaptive security responses.

PROPOSED SYSTEM

The proposed system introduces an intelligent and adaptive cloud security framework that integrates machine learning–driven multi-factor authentication with dynamic cryptographic agility. Unlike traditional static models, the system evaluates contextual signals, behavioral patterns, and threat intelligence in real time to determine authentication and encryption requirements.

Authentication is treated as a continuous process rather than a one-time event. Machine learning models analyze login behavior, device fingerprints, geolocation data, and session activity to assign dynamic risk scores. Based on the assessed risk level, the system enforces adaptive MFA and adjusts cryptographic strength accordingly.

The framework also integrates anomaly detection and intrusion monitoring with authentication workflows, enabling proactive defense mechanisms such as step-up authentication, encryption escalation, or session termination when suspicious behavior is detected.

Advantages of Proposed System

1. **Dynamic and Risk-Adaptive Authentication**
   Authentication requirements are adjusted in real time based on machine learning–driven risk assessment.
2. **Continuous User Verification**
   Session behavior is continuously monitored to detect hijacking attempts and insider threats.
3. **Adaptive Cryptography and Crypto Agility**
   Encryption algorithms and key parameters dynamically adjust based on data sensitivity and threat level.
4. **Improved Detection Accuracy**
   Machine learning reduces false acceptance and false rejection rates by distinguishing legitimate users from attackers more effectively.
5. **Integrated and Unified Security Architecture**
   Authentication, anomaly detection, and encryption operate as a coordinated security ecosystem, improving overall cloud resilience.

IV. RESULTS AND DISCUSSIONS

Experimental Setup

The proposed cloud security framework was evaluated in a simulated cloud environment designed to replicate real-world authentication scenarios. The system was tested under varying user loads, device contexts, and threat conditions to assess authentication accuracy, risk detection capability, encryption overhead, and scalability.

Both legitimate and attack-oriented authentication requests were generated, including credential stuffing attempts, abnormal login behaviors, replay patterns, and session hijacking simulations. Performance metrics such as authentication accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), detection latency, and system throughput were analyzed.

1. Authentication Accuracy and Risk Classification

The integration of machine learning significantly improved authentication decision accuracy compared to traditional static MFA systems. Behavioral and contextual feature analysis enabled precise classification of login attempts as legitimate or suspicious.

- Authentication Accuracy achieved high performance due to behavioral modeling.
- False Acceptance Rate (FAR) was reduced through anomaly detection.
- False Rejection Rate (FRR) was minimized by contextual risk analysis.
- Risk-based authentication reduced unnecessary MFA prompts for low-risk users.

2. Performance of Adaptive Multi-Factor Authentication

The adaptive MFA mechanism demonstrated efficient operation under both normal and high-risk scenarios.

- Low-risk login attempts were processed seamlessly without additional verification steps.
- High-risk attempts triggered step-up authentication, including additional verification factors.
- Authentication latency remained within acceptable limits even during peak loads.
- Selective MFA enforcement reduced overall system overhead compared to static MFA systems.

3. Machine Learning–Based Attack Detection

The ML-based anomaly detection module effectively identified multiple attack scenarios:

2250-3676 ijesatj@gmail.com https://www.ijesat.com/

International Journal of Engineering Science and Advanced Technology (IJESAT)
Vol 26 Issue 02(February),2026
Received: 08-01-2026 Accepted: 17-02-2026 Published: 24-02-2026

- Credential stuffing attempts were detected based on abnormal login frequency patterns.
- Replay attacks were identified through session inconsistency signals.
- Session hijacking was detected using continuous behavioral monitoring.
- Suspicious device and location changes triggered real-time alerts.

The predictive attack detection capability allowed preventive action before successful account compromise. Continuous model learning further improved detection performance over time.

4. Adaptive Cryptography Evaluation

The adaptive cryptographic module dynamically selected encryption algorithms and key strengths based on assessed risk levels.

- High-risk sessions invoked stronger encryption configurations.
- Low-risk operations utilized lightweight encryption to optimize performance.
- Encryption switching occurred without disrupting user sessions.
- Cryptographic agility reduced exposure to static algorithm vulnerabilities.

Performance analysis showed that adaptive cryptography maintained high data protection while minimizing computational overhead under large-scale conditions.

5. Scalability and Load Handling

Scalability tests were conducted by increasing concurrent authentication requests and session activity levels.

- The system maintained stable throughput under heavy load conditions.
- Machine learning inference time remained consistent with minimal delay.
- Cryptographic operations were efficiently optimized for cloud deployment.
- Resource utilization remained balanced across modules.

These results confirm that the proposed framework is suitable for large-scale cloud environments with dynamic workloads.

6. Security Analysis Against Common Threats

The proposed framework was evaluated against major cloud security threats:

- Credential stuffing attacks were mitigated through anomaly detection and adaptive MFA.
- Replay attacks were prevented using secure session handling and nonce validation.
- Man-in-the-middle attacks were blocked through strong encryption protocols.
- Session hijacking attempts were neutralized via continuous authentication monitoring.

Compared to traditional systems, the integrated approach demonstrated stronger resistance to both external and insider threats.

V. CONCLUSION & FUTURE SCOPE

The rapid expansion of cloud computing has significantly increased the complexity of securing user identities, sensitive data, and distributed infrastructures. Traditional authentication mechanisms and static cryptographic configurations are no longer sufficient to defend against sophisticated and adaptive cyber threats. This work presented an intelligent cloud security framework that integrates machine learning–driven multi-factor authentication with adaptive cryptographic agility to enhance protection in modern cloud environments.

The proposed system moves beyond rule-based authentication by incorporating behavioral analysis, contextual risk assessment, and continuous monitoring. Machine learning models dynamically evaluate login attempts and session activities, assigning risk scores that determine the required level of authentication and encryption strength. This adaptive approach minimizes unnecessary verification for low-risk users while enforcing stronger controls for high-risk scenarios, thereby achieving a balance between security and usability.

Furthermore, the integration of adaptive cryptography ensures dynamic selection of encryption algorithms and key parameters based on threat conditions and data sensitivity. The unified coordination between authentication, anomaly detection, and encryption mechanisms strengthens resistance against credential stuffing, replay attacks, session hijacking, and impersonation attempts. Experimental observations confirm improved authentication accuracy, reduced false acceptance rates, and scalable performance under high user loads. Overall, the proposed framework establishes

a resilient, scalable, and future-ready cloud security architecture.

FUTURE SCOPE

Although the proposed system significantly enhances cloud security, several improvements and research extensions can further strengthen its effectiveness:

1. **Integration of Advanced Biometric Modalities**
   Future work can incorporate multimodal biometrics such as facial recognition, voice authentication, and behavioral biometrics derived from mobile sensors to improve authentication accuracy.
2. **Federated and Privacy-Preserving Learning**
   Implementing federated learning can enable distributed model training across cloud environments without exposing sensitive user data, enhancing privacy and compliance.
3. **Explainable Artificial Intelligence (XAI)**
   Incorporating explainable ML models would improve transparency in risk-based authentication decisions and increase user and regulatory trust.

REFERENCES

1. NIST, Special Publication 800-63B: Digital Identity Guidelines—Authentication and Lifecycle Management, National Institute of Standards and Technology.
2. NIST, Special Publication 800-207: Zero Trust Architecture, National Institute of Standards and Technology, 2020.
3. OWASP, "Multifactor Authentication Cheat Sheet," OWASP Cheat Sheet Series
4. OWASP, "Testing Multi-Factor Authentication (MFA)," Web Security Testing Guide.
5. W3C, Web Authentication: An API for Accessing Public Key Credentials (WebAuthn) Level 2, W3C Recommendation, 2021.
6. W3C, Web Authentication: An API for Accessing Public Key Credentials (WebAuthn) Level 3, W3C Technical Report, 2025.
7. FIDO Alliance, "Passkeys: Passwordless Authentication," FIDO Alliance.
8. Microsoft, "Deploy a passwordless replacement option," Microsoft Learn, 2024.
9. Microsoft, "Plan a Windows Hello for Business deployment," Microsoft Learn, 2025.
10. Microsoft, "Passkeys (FIDO2) authentication method in Microsoft Entra ID," Microsoft Learn, 2025.
11. I. Matiushin, "MLE-RBA: A Machine Learning-Empowered Risk-Based Authentication," ACM/Springer proceedings chapter, 2025.
12. P. Bansal et al., "Continuous Authentication in the Digital Age: An Analysis…," Computers, vol. 13, no. 4, 2024.
13. M. Hu et al., "AuthConFormer: Sensor-based Continuous Authentication…," Computers & Security, 2023.
14. J. Saleem et al., "Machine Learning-Enhanced Attribute-Based Authentication…," 2025.
15. NIST, "NIST Releases First 3 Finalized Post-Quantum Encryption Standards," Aug. 13, 2024.
16. NIST CSRC, "Post-Quantum Cryptography FIPS Approved," Aug. 13, 2024.
17. NIST, Considerations for Achieving Crypto Agility, (CSWP 39), 2025.
18. P. R. Kumar et al., "A secure and efficient encryption system based on …," Scientific Reports, 2025.
19. Experts/Repository entry, "High-secure fingerprint authentication system using ring-LWE cryptography…," (ring-LWE + NTT latency results).
20. OWASP, "Authentication Cheat Sheet," OWASP Cheat Sheet Series