STRENGTHENING CLOUD SECURITY WITH MACHINE LEARNING-DRIVEN MULTI-FACTOR AUTHENTICATION AND ADAPTIVE CRYPTOGRAPHY

ABSTRACT

As cloud computing becomes integral to data storage and enterprise operations, ensuring secure user authentication and information transmission is paramount. This study presents a machine learning-driven Multi-Factor Authentication (MFA) system integrated with Adaptive Cryptography to enhance cloud security frameworks. By employing behavioral biometrics, device-level patterns, and dynamic key generation, the proposed approach strengthens both authentication and encryption. The model utilizes ML algorithms to predict anomalous access patterns, while adaptive cryptographic modules automatically modify encryption strategies based on user risk profiles. Experimental evaluations demonstrate superior performance over static authentication systems, achieving enhanced detection accuracy, reduced false positives, and optimized cryptographic efficiency. This intelligent fusion of authentication and encryption ensures confidentiality, integrity, and resilience within next-generation cloud infrastructures.

Keywords: Cloud security, machine learning, multi-factor authentication, adaptive cryptography, anomaly detection, data protection, behavioral biometrics, dynamic encryption.

EXISTING SYSTEM

Existing cloud security models primarily employ static authentication and traditional encryption mechanisms. Password-based or token-based MFA systems verify user identity through fixed credentials or one-time codes but lack adaptability to real-time behavioral variations. These systems rely heavily on user input and predefined access policies, which can easily be compromised by phishing, credential theft, or brute-force attacks.

Similarly, traditional encryption methods use static keys generated during session initialization. Although secure under ideal conditions, these keys remain vulnerable if intercepted or reused. Furthermore, existing frameworks operate reactively—detecting intrusions only after they occur—rather than proactively mitigating threats through predictive analytics.

The current approach, therefore, lacks contextual intelligence and cannot autonomously respond to shifting attack vectors or user behaviors. The absence of AI-driven adaptability reduces their ability to maintain strong security across dynamic cloud infrastructures.

Disadvantages of Existing System

1. Static Authentication: Reliance on fixed passwords or tokens increases vulnerability to credential theft and brute-force attacks.
2. Non-Adaptive Encryption: Static keys and uniform cryptographic policies fail to respond to evolving risk contexts.
3. Low Predictive Capability: Inability to detect or adapt to suspicious user behavior limits proactive threat prevention.

PROPOSED SYSTEM

The proposed Machine Learning-Driven Multi-Factor Authentication with Adaptive Cryptography (ML-MFAAC) model introduces an intelligent, layered security framework that unites adaptive authentication and encryption into a single automated system.

The framework incorporates behavioral analytics, contextual learning, and risk-based encryption, achieving continuous protection without compromising user experience. The ML module analyzes user-specific parameters—keystroke dynamics, geolocation, device usage, and login time—to determine a dynamic risk score. Based on this score, the system automatically adjusts the authentication requirements and encryption strength.

For low-risk users, access is granted using minimal verification, ensuring convenience; for high-risk cases, the system enforces additional biometric verification and higher encryption standards. Adaptive Cryptography dynamically regenerates keys using ML-based randomness and behavior-driven entropy, significantly reducing the risk of key reuse or compromise.

Experimental evaluation using cloud-based authentication logs revealed superior performance compared to traditional methods. The ML-MFAAC framework achieved higher accuracy in detecting abnormal access attempts while maintaining reduced latency in encryption-decryption operations. This hybridized security solution ensures confidentiality, availability, and integrity within AI-augmented cloud infrastructures.

Advantages of Proposed System

1. Behavior-Driven Security: Uses ML-based analytics to adapt authentication and encryption in real time.
2. Dynamic Key Generation: Adaptive cryptography prevents key reuse and enhances encryption robustness.
3. Proactive Threat Detection: Predicts and mitigates suspicious access patterns before breaches occur.

SYSTEM REQUIREMENTS

- **H/W System Configuration:-**
- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS:

- **Operating system** : Windows 7 Ultimate.
- **Coding Language** : Python.
- **Front-End** : Python.
- **Back-End** : Django-ORM
- **Designing** : Html, css, javascript.
- **Data Base** : MySQL (WAMP Server).