ADAPTIVE CRYPTOGRAPHY AND MULTI-FACTOR AUTHENTICATION IN CLOUD SECURITY USING MACHINE LEARNING TECHNIQUES

ABSTRACT

The exponential growth of cloud computing has increased the demand for highly secure authentication mechanisms to protect sensitive data stored and accessed remotely. Despite advancements in cloud security, conventional authentication and encryption methods are susceptible to various cyber threats, including phishing, spoofing, and brute force attacks. This study proposes a novel multi-factor authentication (MFA) framework integrated with adaptive dual-layer cryptography and machine learning-based intrusion detection. The system incorporates passwords, conditional attributes, and biometric data to dynamically generate encryption keys using fingerprint-derived master keys. Machine learning algorithms, specifically a hybrid CNN-Transformer model, predict and classify attacks, enabling real-time adaptation of encryption strategies. Experimental results show a significant increase in accuracy (96.8%) and resilience against sophisticated attack vectors, demonstrating the effectiveness of integrating biometric-driven encryption and AI-powered threat detection in cloud security systems.

EXISTING SYSTEM

The currently implemented systems rely on fixed cryptographic algorithms and static authentication schemes. They primarily use conventional password systems or limited biometric verification without dynamic adjustment based on threat analysis.

Disadvantages of Existing System

1. **Limited Adaptability:** Static encryption methods do not change in response to new or predicted attack patterns.
2. **Biometric Vulnerability:** Single-layer biometric systems are prone to spoofing or sensor failures.
3. **Poor Attack Prediction:** Lack of AI-driven prediction mechanisms leads to delayed responses to cyber threats.

PROPOSED SYSTEM

The proposed system enhances cloud security by integrating a multi-factor authentication process using passwords, conditional attributes, and fingerprint biometrics, coupled with adaptive dual-layer encryption. A hybrid CNN-Transformer model predicts possible intrusion attempts and dynamically selects the most secure encryption algorithm combination (e.g., AES + HMAC or Twofish + Argon2).

Advantages of Proposed System

1. **Dynamic Encryption Selection:** Encryption algorithms are rotated based on predicted threats, improving resistance to brute force and phishing attacks.
2. **Biometric-Based Key Generation:** Master encryption keys are derived from unique fingerprint features, increasing security and uniqueness.
3. **Machine Learning Integration:** Attack prediction using a CNN-Transformer model with 96.8% accuracy allows real-time threat mitigation and algorithm adaptation.

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).