Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

# Adaptive Contextual Token-Biometric Authentication (ACTBA) for Cloud Access: A Novel Two-Factor Security Mechanism

Mrs. G. Krishna Keerthana
Assistant Professor, Department of CSE (AI&ML)
Siddhartha Institute of Technology & Sciences, Hyderabad

Dr. G. Dileep Kumar
Associate Professor, Department of CSE
Siddhartha Institute of Technology & Sciences, Hyderabad.

**Abstract: - The rapid expansion of cloud computing has intensified concerns related to identity security and unauthorized access. Although two-factor authentication (2FA) mechanisms are widely adopted to mitigate risks associated with password compromise, many existing solutions rely on static authentication workflows that fail to adapt to dynamic threat conditions. Such rigidity often results in either weakened security or degraded user experience. To address these limitations, this paper proposes Adaptive Contextual Token-Biometric Authentication (ACTBA), a novel two-factor authentication framework specifically designed for secure cloud access. ACTBA integrates contextual risk assessment, time-synchronized cryptographic tokens, and lightweight biometric verification to dynamically adjust authentication strength based on real-time risk indicators. Formal definitions, mathematical modeling, and security analysis demonstrate that ACTBA provides enhanced resistance against phishing, replay, and credential theft attacks while preserving usability and user privacy. The proposed framework offers a scalable and future-ready authentication solution for modern cloud environments.**

**Keywords: Adaptive Authentication, Cloud Security, Two-Factor Authentication, Context-Aware Security, Biometrics, Identity Management**

## 1. INTRODUCTION:

Cloud computing has become a cornerstone of modern digital ecosystems, enabling organizations to deploy scalable applications and services with minimal infrastructure investment. Despite its advantages, cloud computing introduces complex security challenges, particularly in identity and access management (IAM). Since cloud services are accessible over public networks and shared infrastructures, authentication mechanisms must be resilient against a wide range of cyber threats.

Password-based authentication remains the most commonly used method for cloud access; however, it is widely acknowledged as insufficient in isolation. Password reuse, phishing campaigns, and large-scale credential leaks continue to undermine traditional authentication systems [1], [2]. Two-factor authentication (2FA) strengthens security by requiring additional verification beyond passwords, yet many widely deployed 2FA solutions suffer from their own vulnerabilities.

For instance, SMS-based one-time passwords are susceptible to SIM-swap attacks and signaling vulnerabilities [3], while hardware tokens increase operational costs and reduce usability. Static biometric systems, although effective in identity binding, raise privacy concerns and lack revocability once compromised [4]. Furthermore, most existing 2FA mechanisms apply uniform authentication requirements regardless of user context, ignoring valuable risk indicators such as device trust, geolocation anomalies, and access behavior.

To overcome these limitations, adaptive and context-aware authentication has gained attention as a promising approach [5]. In this work, we introduce **Adaptive Contextual Token-Biometric Authentication (ACTBA)**, which dynamically modifies authentication requirements based on real-time contextual risk assessment. By combining cryptographic tokens with biometric verification under an adaptive framework, ACTBA aims to provide robust cloud access security while maintaining usability and privacy.

## 2. BACKGROUND AND MOTIVATION:

### *2.1 Security Challenges in Cloud Authentication*

Cloud platforms support a diverse set of users, including administrators, employees, third-party vendors, and automated services. This diversity increases the attack surface and makes static authentication policies ineffective. Attackers frequently exploit stolen credentials to gain persistent cloud access, often without triggering alarms [6].

Moreover, cloud access occurs across heterogeneous devices and locations, further complicating authentication decisions. A login attempt from an unfamiliar device or location may pose significantly higher risk than a routine access from a

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

trusted environment, yet traditional authentication mechanisms treat both cases identically.

### *2.2 Limitations of Conventional Two-Factor Authentication*

Existing 2FA approaches primarily focus on adding an extra authentication factor but lack intelligence and adaptability. Key limitations include:

- Dependence on insecure communication channels (e.g., SMS)
- Inability to distinguish between legitimate and suspicious login contexts
- Poor balance between security enforcement and user convenience
- Limited support for privacy-preserving biometric processing

These shortcomings highlight the need for an authentication framework that can dynamically adjust security controls in response to evolving risk conditions.

### *2.3 Motivation for ACTBA*

ACTBA is motivated by the observation that authentication risk is context-dependent rather than static. By incorporating contextual signals and adaptive decision logic, ACTBA strengthens authentication only when necessary, thereby reducing unnecessary friction for legitimate users while improving security against advanced attacks.

## 3. DEFINITIONS AND PRELIMINARIES:

This section introduces the fundamental concepts and terminologies that form the theoretical basis of the proposed Adaptive Contextual Token-Biometric Authentication (ACTBA) framework. Clearly defining these terms is essential for understanding the design principles, security assumptions, and operational flow of the proposed authentication mechanism.

### *Definition 1: Two-Factor Authentication (2FA)*

Two-Factor Authentication (2FA) is a security mechanism used to verify the identity of a user by requiring two independent and distinct authentication factors. These factors are typically selected from the following three categories:

1. Knowledge factors – something the user knows (e.g., passwords, PINs).
2. Possession factors – something the user has (e.g., hardware tokens, mobile devices, cryptographic keys).
3. Inherence factors – something the user is (e.g., biometric traits such as fingerprints, facial features, or iris patterns).

The core security principle of 2FA lies in the independence of the factors; compromising one factor alone should not be sufficient to gain unauthorized access. Compared to single-factor authentication, 2FA significantly improves resistance against common attacks such as password guessing, phishing, and credential reuse. In cloud environments, 2FA serves as a foundational defense mechanism against identity-based threats while balancing usability and security requirements.

### *Definition 2: Contextual Risk Score*

A Contextual Risk Score is a numerical or probabilistic measure that represents the estimated likelihood of an authentication attempt being malicious or unauthorized. This score is computed by analyzing a set of contextual attributes associated with the access request, including but not limited to:

- Device trust level and fingerprint consistency
- Geographical location and location deviation
- Network characteristics (IP reputation, network type)
- Temporal patterns such as access time anomalies
- User behavioral patterns and historical access profiles

The contextual risk score enables the authentication system to move beyond static decision rules by incorporating real-time situational awareness. Higher risk scores indicate suspicious or abnormal behavior, prompting stricter authentication requirements, while lower scores allow seamless access with minimal friction. In the ACTBA framework, the contextual risk score plays a central role in dynamically selecting the appropriate authentication path.

### *Definition 3: Adaptive Authentication*

Adaptive Authentication refers to an intelligent authentication strategy that dynamically adjusts verification requirements based on real-time risk evaluation rather than enforcing a fixed authentication policy for all users and scenarios. Unlike traditional authentication systems that apply uniform security rules, adaptive authentication continuously evaluates contextual signals to determine the appropriate level of security enforcement.

Key characteristics of adaptive authentication include:

- Risk-based decision making
- Context awareness

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

- Dynamic escalation or relaxation of authentication factors
- Improved balance between security and user experience

By tailoring authentication strength to the assessed risk level, adaptive authentication reduces unnecessary user burden during low-risk access attempts while ensuring robust protection during high-risk scenarios. This approach is particularly well-suited for cloud environments, where access patterns are highly dynamic and users operate across diverse devices and locations.

***Definition 4: Token-Biometric Authentication***

Token-Biometric Authentication is a hybrid authentication mechanism that combines cryptographic token validation with biometric identity verification to achieve stronger user authentication guarantees. In this approach:

- The token factor (possession-based) ensures that the user holds a valid, cryptographically protected credential, such as a one-time token or device-bound key.
- The biometric factor (inherence-based) verifies the user's physiological or behavioral identity traits, ensuring that the legitimate owner of the token is present.

The integration of token-based and biometric authentication mitigates the limitations of each individual factor. While tokens can be lost or stolen, biometric verification prevents misuse. Conversely, token validation adds an additional security layer that protects against biometric spoofing or replay attacks. In the proposed ACTBA framework, token-biometric authentication is adaptively enforced based on contextual risk, enhancing both security robustness and privacy preservation.

## 4. ACTBA SYSTEM ARCHITECTURE:

This section presents the architectural design of the Adaptive Contextual Token-Biometric Authentication (ACTBA) framework. The proposed architecture is designed to provide strong security guarantees while maintaining usability, scalability, and compatibility with modern cloud identity and access management (IAM) infrastructures. By adopting a modular and loosely coupled design, ACTBA supports adaptive decision-making, privacy preservation, and seamless integration across heterogeneous cloud environments.

### *4.1 Overview of the ACTBA Framework*

The ACTBA framework is structured around five interconnected functional modules, each responsible for a distinct aspect of the authentication process. The interaction among these modules enables real-time risk-aware authentication that dynamically adapts security requirements based on contextual conditions.

#### *4.1.1 Authentication Gateway (AG)*

The Authentication Gateway (AG) serves as the primary entry point for all user authentication requests to the cloud system. It acts as an interface between end users and backend authentication services. The AG is responsible for collecting initial authentication credentials, contextual metadata (such as device identifiers, IP address, and access timestamps), and routing the request to the appropriate internal modules.

In addition to request routing, the AG enforces preliminary access control checks, validates request integrity, and ensures secure communication using standard cryptographic protocols. By centralizing authentication entry points, the AG simplifies policy enforcement and enables consistent security monitoring across cloud services.

#### *4.1.2 Contextual Risk Engine (CRE)*

The Contextual Risk Engine (CRE) is the intelligence core of the ACTBA framework. It evaluates a wide range of contextual parameters associated with each authentication attempt and computes a real-time contextual risk score. These parameters may include device trust level, geographic location consistency, network characteristics, historical user behavior, and temporal access patterns.

The CRE leverages risk assessment models to detect anomalies and deviations from normal user behavior. By quantifying risk rather than relying on static rules, the CRE enables fine-grained and adaptive authentication decisions. This risk-centric design is essential for addressing evolving threats such as credential theft, account takeover, and insider misuse in cloud environments.

#### *4.1.3 Token Generation Module (TGM)*

The Token Generation Module (TGM) is responsible for generating cryptographically secure, time-synchronized authentication tokens that serve as a possession-based factor. These tokens are dynamically generated and bound to trusted user devices, reducing the risk of replay attacks and unauthorized reuse.

The TGM supports short-lived token validity and device binding mechanisms, ensuring that tokens remain usable only within a limited temporal and contextual scope. By integrating token generation into the adaptive authentication workflow, ACTBA strengthens security during medium- and high-risk access attempts without imposing unnecessary overhead on low-risk users.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

#### *4.1.4 Biometric Verification Module (BVM)*

The Biometric Verification Module (BVM) performs user identity verification using biometric traits such as fingerprints or facial features. To address privacy concerns, the BVM employs privacy-preserving biometric processing techniques, ensuring that raw biometric data is neither stored nor transmitted in an identifiable form.

Instead of direct biometric templates, secure feature representations or encrypted biometric hashes are used during verification. The BVM is activated selectively based on the risk assessment outcome, allowing biometric authentication to be enforced only when elevated assurance is required. This selective activation reduces user friction while maintaining strong protection against impersonation and credential compromise.

#### *4.1.5 Decision Engine (DE)*

The Decision Engine (DE) orchestrates the overall authentication workflow by determining the appropriate authentication path based on the contextual risk score produced by the CRE. It applies predefined risk thresholds and adaptive policies to decide whether an authentication attempt requires:

- Token-based verification only
- Combined token and biometric verification
- Additional security checks or access denial

By decoupling decision logic from individual authentication components, the DE enables flexible policy updates and supports organization-specific security requirements. This adaptability is crucial for cloud environments where threat models, compliance obligations, and user behaviors continuously evolve.

### 4.2 Architectural Benefits

The modular design of the ACTBA framework offers several advantages:

- Scalability: Independent modules allow horizontal scaling to support large user populations.
- Interoperability: The architecture can integrate with existing cloud IAM platforms with minimal modification.
- Security Adaptability: Risk-aware decision-making enhances resilience against sophisticated attacks.
- Privacy Preservation: Biometric data is protected through selective activation and secure processing.

Overall, the ACTBA system architecture establishes a robust foundation for adaptive, privacy-aware, and context-sensitive authentication in cloud computing environments.

## 5. MATHEMATICAL MODELING:

### *5.1 Contextual Risk Assessment*

The contextual risk score $R$is computed as:

$$R = \sum_{i=1}^{n} w_i \cdot C_i$$

where $C_i$represents normalized contextual factors such as device deviation, geolocation anomaly, time irregularity, and behavioral deviation, and $w_i$denotes the corresponding weight assigned to each factor, with $\sum w_i = 1$.

### *5.2 Authentication Decision Thresholds*

Three risk thresholds guide the adaptive authentication process:

- $R < T_1$: Low-risk authentication
- $T_1 \leq R < T_2$: Medium-risk authentication
- $R \geq T_2$: High-risk authentication

### *5.3 Token Generation Mechanism*

ACTBA employs a cryptographic token generated as:

$$Token = HMAC(K_u, T \parallel D)$$

where $K_u$is a user-specific secret key, $T$is a time window, and $D$represents device fingerprint data. This ensures token freshness and device binding.

## 6. SECURITY ANALYSIS:

ACTBA is resilient against multiple attack vectors:

- **Phishing Attacks:** Stolen credentials alone are insufficient due to token and biometric requirements.
- **Replay Attacks:** Time-bounded tokens prevent reuse of captured authentication messages.
- **Man-in-the-Middle Attacks:** Cryptographic token validation ensures message integrity.
- **Biometric Spoofing:** Support for liveness detection and multi-modal verification reduces spoofing risks [4].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 02 , February - 2026

## 7. COMPARATIVE ANALYSIS:

| **Authentication Scheme** | **Adaptivity** | **Security Level** | **Usability** | **Privacy** |
|---|---|---|---|---|
| Password-Only | No | Low | High | Medium |
| Static 2FA | No | Medium | Medium | Medium |
| Biometric-Only | No | Medium | High | Low |
| **ACTBA** | **Yes** | **High** | **High** | **High** |

## 8. CONCLUSION:

This paper presented **Adaptive Contextual Token-Biometric Authentication (ACTBA)**, a novel two-factor authentication framework designed for secure and intelligent cloud access. By integrating contextual risk assessment, cryptographic token generation, and biometric verification, ACTBA addresses the limitations of static authentication mechanisms. The proposed framework enhances resistance against modern attack vectors while preserving usability and user privacy. ACTBA represents a significant step toward adaptive, user-centric authentication for next-generation cloud environments.

## REFERENCES:

[1] P. Mell and T. Grance, “The NIST definition of cloud computing,” NIST, 2011.
[2] J. Bonneau et al., “The quest to replace passwords,” *IEEE Security & Privacy*, 2012.
[3] F. Aloul, “Two-factor authentication using mobile phones,” *IEEE CCA*, 2009.
[4] A. K. Jain, A. Ross, and K. Nandakumar, *Introduction to Biometrics*, Springer, 2016.
[5] K. Nguyen, “Context-aware authentication in cloud environments,” *IEEE TSC*, 2020.
[6] S. Subashini and V. Kavitha, “Security issues in cloud computing,” *Journal of Network and Computer Applications*, 2011.
[7] A. Das et al., “Security analysis of SMS-based authentication,” *ACM CCS*, 2014.
[8] P. Reddy et al., “Adaptive authentication for cloud services,” *Journal of Cloud Computing*, 2021.