International Journal of Cybersecurity, Digital Systems and Technologies
IJCDST : Sep - Dec 2026 | Vol. 1 No. 3 (2026)

A Secure Authentication Framework for Protecting Digital Identity in Cloud-Based Systems

Farrukh Aslam Khan,

Professor, Department of Computer Science, King Saud University, Saudi Arabia

Abstract

Cloud computing has become an essential technology for storing information, delivering digital services, and supporting remote access to organizational resources. However, the increasing dependence on cloud platforms has introduced security challenges related to identity theft, unauthorized access, credential compromise, and account hijacking. Traditional authentication methods that depend mainly on usernames and passwords may not provide sufficient protection against phishing, credential reuse, and automated attacks. This paper proposes a secure authentication framework for protecting digital identity in cloud-based systems. The framework integrates multi-factor authentication, risk-based access verification, identity lifecycle management, encrypted communication, and continuous access monitoring. It evaluates contextual information, including device characteristics, login location, access patterns, and authentication history, to identify potentially suspicious access attempts. The proposed approach also incorporates secure session management, least-privilege access control, and privacy-aware identity data handling. The paper presents the framework architecture, operational workflow, implementation considerations, evaluation methodology, and potential limitations. The proposed framework offers a structured foundation for improving digital identity protection in cloud environments while balancing security, usability, and operational efficiency.

Keywords: *Cloud computing, digital identity, secure authentication, multi-factor authentication, access control, identity management, cybersecurity.*

Received : 08.09.2026 | **Acceptance :** 12.09.2026 | **Publication :** 15.09.2026

1. Introduction

Cloud computing has transformed the way organizations manage digital resources, applications, databases, and information systems. Organizations increasingly use cloud-based platforms to support remote working, online transactions, collaboration, and data sharing. These services provide flexibility, scalability, and convenient access to information from different locations and devices. However, the same accessibility creates security challenges when digital identities are inadequately protected.

Digital identity represents the information used to identify a person, device, application, or service within a digital environment. Authentication verifies whether an entity controls the credentials or authenticators associated with a claimed identity. Authorization determines which resources that authenticated entity is permitted to access. Both functions are essential because a compromised identity can provide an attacker with access to confidential information, business applications, and administrative resources.

Traditional authentication systems commonly rely on passwords. Although passwords are widely used and relatively simple to implement, they are vulnerable to phishing, credential stuffing, brute-force attacks, password reuse, and social engineering. Attackers may also obtain credentials through data breaches or malicious software. When the same credentials are reused across multiple services, the compromise of one account may expose additional accounts.

Multi-factor authentication (MFA) strengthens account protection by requiring evidence from more than one authentication factor. However, not all MFA methods provide the same level of security. One-time codes and push notifications can remain vulnerable to phishing, social engineering, or authentication fatigue. Consequently, cloud security requires a broader approach that combines strong authentication with contextual risk assessment, secure session management, identity lifecycle controls, and continuous monitoring.

Zero-trust security principles further emphasize that access should be granted according to verified identity, device conditions, resource sensitivity, and applicable access policies rather than assumed trust based on network location alone (Rose et al., 2020). This principle is particularly relevant to cloud environments where users and services interact across distributed infrastructure.

This paper proposes a secure authentication framework designed to protect digital identities throughout the access process. The framework combines identity verification, adaptive authentication, policy-based authorization, session protection, and suspicious-activity monitoring. Its objective is to provide a practical security architecture that reduces the risk of unauthorized access while maintaining a manageable authentication experience for legitimate users.

2. Related Work

Digital identity protection has received considerable attention in cybersecurity research and standards development. Existing approaches address authentication assurance, credential management, access control, and secure communication through complementary mechanisms.

The National Institute of Standards and Technology (NIST) provides digital identity guidance covering authentication requirements, authenticator management, and identity-related security controls. These guidelines emphasize selecting authentication mechanisms according to the level of risk and the assurance required by a particular application (NIST, 2025). They provide an important foundation for designing authentication systems that are more secure than password-only mechanisms.

Multi-factor authentication is widely used to reduce the consequences of compromised passwords. It combines multiple types of evidence, such as knowledge, possession, and inherence. Nevertheless, its effectiveness depends on the selected methods and implementation. Phishing-resistant authenticators, including suitable public-key-based authentication mechanisms, can provide stronger protection than methods that rely on manually entered codes.

The Web Authentication specification developed by the World Wide Web Consortium supports public-key-based authentication through authenticators that can be integrated with browsers and web applications (W3C, 2021). When implemented correctly, these mechanisms can reduce exposure to credential phishing because authentication is bound to the legitimate service's origin.

OAuth 2.0 and OpenID Connect also contribute to cloud identity management. OAuth 2.0 supports delegated authorization, while OpenID Connect provides an identity layer for authentication and user information. However, secure deployment requires careful handling of redirect URIs, tokens, client credentials, and authorization flows. Current OAuth security guidance recommends measures intended to reduce risks such as authorization-code interception and misuse of access tokens (Lodderstedt et al., 2025).

Zero-trust architecture provides an additional perspective by requiring access decisions to be based on explicit policy evaluation and relevant security information. Rather than assuming that a successfully authenticated user should receive unrestricted access, the architecture evaluates whether the requested resource and operation are appropriate for that identity and context (Rose et al., 2020).

Although these approaches address important security requirements, practical deployments may still face challenges involving inconsistent identity policies, weak recovery procedures, excessive permissions, stolen sessions, and limited visibility into suspicious login activity. The proposed

framework integrates these complementary controls into a single authentication workflow, with particular emphasis on risk-based verification and secure identity lifecycle management.

3. Problem Statement and Research Objectives

The principal problem addressed in this study is the difficulty of maintaining reliable digital identity protection across cloud applications accessed by users, devices, and services from different locations. Password-based authentication alone cannot adequately address all threats associated with credential theft, phishing, compromised devices, and unauthorized session use.

Furthermore, adding authentication steps indiscriminately can negatively affect usability and productivity. A practical framework should therefore apply stronger verification when the context indicates increased risk while avoiding unnecessary interruptions during routine, low-risk access.

The objectives of this study are to design a secure authentication framework for cloud-based systems, integrate multi-factor authentication and risk-based verification, strengthen session and token protection, and establish appropriate authorization and identity lifecycle controls. The study also proposes an evaluation methodology for assessing authentication security, false rejection rates, access latency, and usability.

The proposed framework is intended to complement existing cloud security mechanisms. It does not assume that authentication alone can prevent every form of cyberattack. Instead, it treats identity verification as one component of a broader security process that includes authorization, monitoring, incident response, and data protection.

4. Proposed Secure Authentication Framework

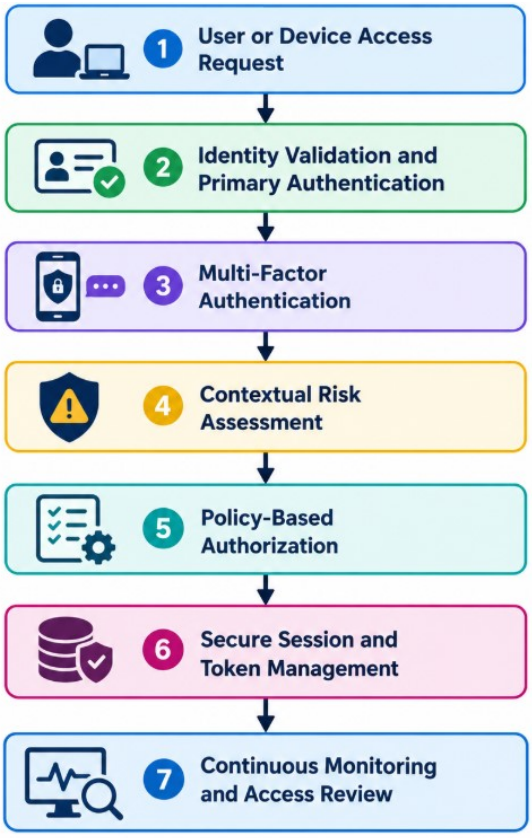


Figure 1. Proposed secure authentication framework

4.1 Framework Architecture

The proposed framework consists of six major components: identity registration and management, primary authentication, multi-factor verification, contextual risk assessment, policy-based authorization, and session monitoring.

The identity management component maintains user accounts, registered authenticators, account status, and assigned roles. The primary authentication component validates the user's initial authentication request. Multi-factor verification provides additional evidence when required by the security policy. The risk assessment component evaluates relevant contextual information, while the authorization component determines the resources and operations permitted to the authenticated identity. Finally, session monitoring identifies suspicious activity after access has been granted.

If authentication fails or a request violates a mandatory security policy, access is denied or restricted. If additional risk is identified, the framework can request stronger authentication, require administrator review, or temporarily block the request. Successful authentication does not automatically grant access to every resource; authorization is evaluated separately for the requested operation.

The architecture can be integrated with cloud applications, centralized identity providers, enterprise directories, and application programming interfaces. Standardized identity protocols can support interoperability, provided that tokens, cryptographic keys, redirect endpoints, and application configurations are managed securely.

4.2 Identity Registration and Lifecycle Management

Secure authentication begins before the first login. The identity registration process should verify the user's identity to a level appropriate for the application and establish an authorized account through a controlled procedure. The organization should prevent duplicate accounts, unauthorized registrations, and inappropriate privilege assignments.

Each account should have a defined owner, role, status, and set of permitted resources. Authentication methods must be registered through a secure process, and changes to sensitive account attributes should require appropriate verification.

Identity lifecycle management includes account creation, credential registration, role changes, temporary suspension, and account removal. When employees leave an organization or a contractor's assignment ends, access should be revoked promptly. Dormant accounts and unused authenticators should be reviewed according to organizational policy.

Account recovery requires particular attention because attackers may bypass strong login protections by exploiting weak recovery procedures. Recovery should not depend exclusively on easily obtained personal information or insecure email access. High-risk recovery requests should require additional verification, appropriate notifications, and, where necessary, administrative review.

4.3 Multi-Factor Authentication

The framework incorporates multi-factor authentication to strengthen verification beyond a password. Authentication factors generally include something the user knows, something the user possesses, and something the user is.

Examples include passwords, hardware security keys, authenticator applications, and biometric verification through supported devices. A biometric characteristic should not be treated as a universally interchangeable secret; its security depends on the authenticator design, device protection, and verification process.

Where supported, phishing-resistant authentication using appropriately configured public-key credentials is preferred for sensitive applications and administrative accounts. Such methods can

reduce dependence on passwords and improve protection against credential replay and fraudulent websites.

The framework should also protect the authentication process against brute-force attempts and automated credential testing. Appropriate measures include rate limiting, suspicious-attempt detection, secure credential storage, and notifications of unusual account activity. Rate limits should be designed carefully to avoid enabling attackers to lock out legitimate users repeatedly.

MFA policies should reflect application sensitivity and user risk. Administrative access, financial operations, and access to highly confidential records may require stronger authentication than routine access to low-risk information. The selected controls should follow recognized security guidance and the organization's threat model.

4.4 Contextual Risk-Based Authentication

Risk-based authentication evaluates relevant contextual information to determine whether an authentication request requires additional verification. The framework may consider device familiarity, login frequency, approximate geographic consistency, network reputation, access time, previous authentication failures, and the sensitivity of the requested resource.

For example, a user logging in from a previously registered device and following a familiar access pattern may complete the normal authentication process. A request involving an unfamiliar device, repeated failed attempts, and an unusual attempt to access administrative resources may require stronger verification.

The risk assessment component assigns a risk category based on the available indicators and defined organizational policies. A low-risk request can proceed when all mandatory requirements are satisfied. A medium-risk request may require additional verification, while a high-risk request may be denied or referred for investigation.

Contextual signals must be interpreted carefully. An unfamiliar location does not necessarily indicate malicious activity because users may travel or use corporate virtual private networks. Similarly, a familiar device may already be compromised. Consequently, contextual assessment should supplement strong authentication rather than replace it.

Risk decisions should be explainable and auditable. The framework should record the relevant security indicators, policy decision, and resulting action without unnecessarily collecting personal information. Periodic review of risk rules can help identify inaccurate decisions and changing attack patterns.

4.5 Authorization and Least-Privilege Access

After authentication, the framework evaluates the requested operation against authorization policies. Role-based access control can assign permissions according to organizational responsibilities, while attribute-based access control can consider factors such as resource classification, device compliance, and the purpose of access.

The principle of least privilege requires users and services to receive only the permissions necessary for their assigned tasks. Ordinary users should not automatically receive administrative privileges, and service accounts should not possess broad access simply because it simplifies application integration.

Sensitive operations may require additional controls even when the user has an established session. Examples include exporting large amounts of data, changing security settings, creating privileged accounts, or modifying access policies. Reauthentication or additional approval may be appropriate for these operations.

Authorization policies should be consistently enforced across cloud applications and APIs. A secure login process is insufficient if individual services fail to validate permissions or accept

unauthorized requests. Centralized policy management and regular permission reviews can reduce inconsistent access decisions.

4.6 Secure Session and Token Management

Authentication systems must protect users after the initial login. An attacker who steals a valid session cookie or access token may gain access without repeating the authentication process. Session security is therefore a necessary part of digital identity protection.

The framework should use secure transport through correctly configured HTTPS connections and protect session identifiers from unnecessary exposure. Browser-based session cookies should use appropriate security attributes, including Secure, HttpOnly, and suitable SameSite settings. Session identifiers should be regenerated when appropriate, particularly after authentication or privilege changes.

Access tokens should have limited lifetimes and narrowly defined permissions. Refresh tokens should be protected against theft and misuse, with rotation or revocation mechanisms selected according to the deployment requirements. Tokens must not be exposed through URLs, public logs, or insecure client storage.

Sessions should expire after defined periods of inactivity or according to application sensitivity. The framework should also support session revocation when an account is disabled, credentials are compromised, or suspicious activity is confirmed. These measures reduce the period during which stolen credentials or session artifacts can be exploited.

5. Implementation Methodology and Evaluation

5.1 Implementation Approach

The proposed framework can be implemented using a cloud identity provider integrated with web applications, centralized policy enforcement, and a security event monitoring system. Standard authentication and federation protocols should be selected according to the application's requirements and supported infrastructure.

The implementation process begins by identifying protected resources, user categories, authentication requirements, and relevant threats. Next, the organization configures identity registration, MFA, authorization policies, session controls, and account recovery procedures. Monitoring rules are then established to identify suspicious authentication attempts and policy violations.

A pilot deployment should be conducted before organization-wide adoption. During the pilot, the security team can evaluate compatibility, user experience, recovery processes, access-denial patterns, and operational performance. Identified problems should be addressed before extending the framework to additional applications.

5.2 Evaluation Metrics

The framework should be assessed using security, performance, and usability metrics. Relevant measures include successful unauthorized-access prevention under defined test scenarios, MFA challenge completion rate, false rejection rate, authentication latency, account recovery success, and the time required to revoke compromised sessions.

The evaluation should include scenarios involving stolen passwords, repeated login failures, phishing attempts, unfamiliar devices, compromised session tokens, and unauthorized privilege escalation. Each scenario should have a clearly defined expected outcome so that the results can be evaluated consistently.

A comparison can be conducted between password-only authentication, conventional MFA, and the proposed risk-based framework. The comparison should use the same application environment and equivalent test conditions. Where risk-based authentication is used, the

evaluation should examine both security outcomes and the additional burden placed on legitimate users.

5.3 Proposed Evaluation Table

Table 1. Evaluation plan for the proposed framework

Evaluation area	Measurement	Purpose
Authentication security	Unauthorized attempts blocked	Assess access protection
MFA effectiveness	Verification success and failure	Examine additional verification
Risk assessment	False-positive and false-negative rates	Evaluate risk classification
Performance	Authentication response time	Measure operational efficiency
Session protection	Unauthorized reuse of revoked sessions	Assess session revocation
Usability	Legitimate login completion rate	Examine user experience

The table defines the proposed evaluation criteria rather than reporting experimental findings. Actual results should be calculated from controlled testing and documented before the framework's effectiveness is claimed.

6. Discussion

The proposed framework integrates several security controls that address different stages of the authentication and access process. Multi-factor authentication strengthens identity verification, contextual risk assessment helps identify suspicious requests, and least-privilege authorization limits the resources available to an authenticated identity. Session monitoring and token protection address risks that continue after login.

An important advantage of this approach is its adaptability. Security policies can be adjusted according to application sensitivity, user responsibilities, and observed threats. Phishing-resistant authentication can be prioritized for privileged users, while additional verification can be requested when a login exhibits unusual characteristics.

However, the framework also introduces implementation challenges. Integrating multiple applications and identity providers may require changes to existing authentication workflows. Incorrectly configured policies can deny legitimate access, while poorly calibrated risk assessment can generate excessive alerts. Organizations must therefore test the framework under realistic operating conditions and review its decisions periodically.

Privacy is another important consideration. Device information, login locations, and access histories may contain sensitive personal data. Collection should be limited to information necessary for security purposes, protected by access controls, and retained according to documented policies. Users should receive appropriate information about monitoring practices where required by applicable law.

The framework also depends on the security of its underlying identity provider. If administrative credentials, signing keys, or identity-provider infrastructure are compromised, attackers may bypass several downstream protections. Strong administrator authentication, separation of duties, key protection, independent logging, and tested incident-response procedures remain essential.

Finally, authentication cannot prevent every attack. Malware operating on an authenticated device, malicious insiders, application vulnerabilities, and compromised third-party services may create risks even when identity verification functions correctly. The proposed framework should

therefore operate as part of a broader cloud security strategy that includes endpoint protection, vulnerability management, encryption, backup, and incident response.

7. Conclusion and Future Work

This paper proposed a secure authentication framework for protecting digital identity in cloud-based systems. The framework combines identity lifecycle management, multi-factor authentication, contextual risk assessment, policy-based authorization, secure session handling, and continuous monitoring. Its central objective is to reduce the risk of unauthorized access while maintaining a practical authentication experience for legitimate users.

The proposed architecture emphasizes that successful authentication should not automatically grant unrestricted access. Access decisions should reflect user identity, requested resources, applicable policies, and relevant security conditions. Phishing-resistant authentication, least-privilege permissions, secure token handling, and reliable account recovery are important elements of this approach.

Future work should implement the framework in a controlled cloud environment and compare it with conventional authentication approaches using measurable security and usability outcomes. Further studies may examine adaptive risk models, passwordless authentication, cross-cloud identity federation, privacy-preserving contextual analysis, and automated detection of compromised sessions.

The proposed framework provides a foundation for designing more resilient identity protection in cloud-based digital systems. Its effectiveness must be established through reproducible testing, careful policy evaluation, and assessment under realistic security conditions.

References

1. *National Institute of Standards and Technology. (2025).* Digital Identity Guidelines: Authentication and Authenticator Management (NIST SP 800-63B-4). *U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63B-4*
2. *Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020).* Zero Trust Architecture (NIST Special Publication 800-207). *National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207*
3. *World Wide Web Consortium. (2021).* Web Authentication: An API for accessing public key credentials—Level 2. *W3C Recommendation. https://www.w3.org/TR/webauthn-2/*
4. *Lodderstedt, T., Bradley, J., Labunets, A., & Fett, D. (2025).* Best Current Practice for OAuth 2.0 Security (RFC 9700). *Internet Engineering Task Force. https://doi.org/10.17487/RFC9700*
5. *National Institute of Standards and Technology. (2020).* Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53, Revision 5). *U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5*
6. *National Institute of Standards and Technology. (2017).* Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). *U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-63b*