2025 Volume: 01 Issue: 06 www.ijrpa.com ISSN 2456-9995 Review Article

International Journal Research Publication Analysis

Page: 01-09

PROPOSING A COMPARATIVE ANALYSIS OF USER AUTHENTICATION TECHNIQUES IN CLOUD SERVICES

***Devashish Sharma, Dr.Vishal Shrivastava, Dr. Akhil Pandey**

Computer Science & Engineering, Arya College of Engineering & I.T. Jaipur, India.

Article Received: 21 October 2025
Article Revised: 10 November 2025
Published on: 30 November 2025

***Corresponding Author: Devashish Sharma**
Computer Science & Engineering, Arya College of Engineering & I.T. Jaipur, India. DOI: https://doi-doi.org/101555/ijrpa.7768

ABSTRACT

This paper analyzes existing user authentication methods in cloud computing, spurred by increased cyber attacks and demands for secure and convenient methods. It assesses a variety of methods from single-factor to advanced multi-factor, passwordless, and adaptive types based on design, security, workflow, and vulnerabilities. Comparative analysis compares each method on security, usability, performance, scalability, and cost. Research findings and technical analysis identify the most appropriate authentication solutions for different cloud services. The findings are that advanced, context-aware, and passwordless methods provide the best balance between security and user convenience. Finally, the paper touches on future innovations, specifically the application of machine learning and AI in creating more intelligent authentication methods.

INTRODUCTION

The cloud computing revolution has radically transformed the information technology landscape through instant access to computing resources. Different services, such as Infrastructure-as-a-Service (IaaS) and Software-as-a-Service (SaaS), now handle massive amounts of sensitive and mission-critical data. The guarantee of strict security in cloud computing environments has therefore become a core concern for users and providers. At the core of cloud security is user authentication, a process of verifying the identity of the user requesting access to cloud services.

In the past, user authentication has largely been based on password-based systems. Those techniques are, however, increasingly recognized for their multiple vulnerabilities. Passwords

are susceptible to all kinds of attacks such as dictionary and brute-force attacks, credential stuffing, and social engineering techniques such as phishing. In addition, the inherent static nature of passwords, combined with the reality that users persist in using weak credentials, leaves massive security vulnerabilities that are continuously exploited by attackers.

This research posits that the application of classical models of authentication is unsuitable for protecting modern cloud infrastructures. Instead, there is a critical need to adopt new and effective forms of authentication. The primary aim of this research is to move beyond simplistic explanations and present an inclusive, comparative overview of different authentication methods within the cloud computing paradigm.

The objectives of this research are as follows:

1. To monitor and document the development of user authentication techniques, from the classical forms to the most advanced techniques being employed currently.
2. In order to compare the design and operational premises underpinning each method, with specific reference to their security models and specifications.
3. In order to perform a critical comparison of these techniques against main performance indicators like security, usability, efficiency, scalability, and cost.

This paper seeks to provide practical suggestions that help cloud service providers and organizations select and deploy the most suitable authentication methods that suit their unique needs. Through these goals, this paper hopes to be a valuable contribution to learning and propelling the adoption of secure, effective, and innovative authentication technologies for cloud-based systems.

Background and Related Work

User verification verifies identity on the basis of three factors: what the user knows (password), they possess (token), and they are (biometric). Methods have moved from one-factor passwords to sophisticated multi-factor and passwordless methods.

Early studies focused on cryptographic techniques for securely storing and transmitting passwords through mechanisms such as hashing and salting to provide additional security. With increased computing power, brute-force attacks became more potent, calling for stronger defense. Multi-Factor Authentication (MFA) played a critical role. Kumar et al.

(2018) studies reveal that MFA is far more effective at blocking unauthorized access than one-factor authentication, especially in preventing account takeovers.

The evolution of cloud computing and the internet increased the necessity for efficient identity management, prompting the introduction of Single Sign-On (SSO) protocols. SAML and OIDC have been the subject of much research. Sun et al. (2019) performed a security analysis of the protocols, taking into account token exchange complexities and risks from insecure identity providers. Research is also concerned with the human aspect of authentication. Frustration with default methods by users leads to weak or stolen passwords, which lower security. This has encouraged the development of passwordless systems. The FIDO Alliance, via FIDO2 and WebAuthn standards, is leading the charge here. Research conducted by Balfanz et al. (2020) indicates that these standards, utilizing public-key cryptography, are more secure and user-friendly.

New advancements have introduced adaptive authentication systems that are AI and machine learning-based. For instance, risk-based authentication (RBA) systems analyze factors like location and device to gauge login risk. On high-risk occasions, users are prompted for extra verification. Mahajan et al. (2021) show that such an approach finds the middle ground between security and user experience. Deep learning models that are often used in medical imaging make a great foundation for advanced RBA solutions. Deep learning models are often used in medical imaging.

These trends are at the center of current user authentication in cloud computing and describe promising future implementation and research areas.

User Authentication Techniques: An In
Depth Technical Review

This chapter gives a technical outline of standard user authentication techniques used in the cloud environment, and explains their design, steps, advantages, and disadvantages.

3.1 Password Authentication

Architecture

Password authentication employs a server to store and authenticate user credentials. It keeps hashed copies with a random salt for every user for added protection instead of plaintext

passwords. The user supplies his password and username, the server extracts the salt, hashes the password, and compares it to the stored hash. If they match, access is provided.

Analysis:

It is a simple method but very vulnerable. It is vulnerable to phishing, dictionary attacks, brute force, and social engineering. It depends on user actions for its security; weak and reused passwords are easily compromised, and it is likely to be the least secure in today's cloud environments.

3.2 MFA

Architecture:

MFA demands at least two different authentication factors to be accessed. Typically, it is a password and something the user possesses, such as an OTP via an app or SMS. The user types in the password first; if correct, they then show a second piece of confirmation, such as a code from their device. Access is granted only after successful verification of both authentication factors.

Analysis:

Multi-Factor Authentication enhances security by introducing additional obstacles for attackers. Although the password may be compromised, the attacker still needs the second factor. But MFA makes the login process more inconvenient and some methods, like SMS codes, vulnerable to attacks like SIM swapping.

3.3 SSO

Architecture:

SSO systems allow users to log in once and access several services. Single Sign-On systems consist of three components: the user, the service provider (SP), and the identity provider (IdP). When a user tries to access a service, the service provider redirects them to the identity provider for authentication. After logging in, the IdP provides a secure token that the SP authenticates before it gives access.

Analysis:

SSO improves user experience by reducing password fatigue and credential management. This is a better way of centralizing the administration of users, but system security relies on the IdP. Connected services are at risk if the IdP is compromised.

3.4 Passwordless Auth

Architecture:

Password-less systems employ public-key cryptography, eliminating passwords. FIDO2 systems allow device registration, creating a custom key pair. The public key remains on the server; the private key remains on the device. The server sends a challenge signed with the private key at authentication, usually accompanied by a biometric or PIN to release. The server verifies the signature using the public key, completing the authentication process.

Analysis: Passwordless authentication enhances security by preventing phishing attacks and eliminating password-related vulnerabilities. It improves user experience by delivering instant, frictionless access on personal devices. Yet also, its uptake depends on compatible hardware and software which is already available. 4.5 Adaptive/Risk-Based Auth (RBA) Architecture: RBA systems adapt authentication according to real-time context. They examine elements such as location, device fingerprinting, and behavioral biometrics. Machine learning can assign risk scores to login attempts, prompting extra verification when the scores are elevated.

Analysis: Adaptive authentication strikes a balance between strong security and user convenience. Low-risk logins are fast, and high-risk instances invoke more stringent controls. Yet, RBA systems are sophisticated and require a huge amount of investment in analytics and data processing.

Service Analysis: A Comparative Evaluation

This contrast compares the strengths and weaknesses of both methods of authentication in terms of security, usability, performance, scalability, and cost of deployment.

4.1 Security Robustness

Password Authentication:

This approach's security relies on the strength of the password chosen by the user and user behavior. Sadly, it's extremely susceptible to current attacks, so it's the least secure approach for cloud infrastructures.

MFA:

MFA provides security through the use of more than one independent factor. Security strength depends on the type of second factor used, with hardware tokens offering greater protection than SMS one-time passwords.

Single Sign-On (SSO):

Single Sign-On remains safe when paired with a trusted Identity Provider, though it introduces a single point of failure. Breaching an IdP breaches all related services.

Passwordless Authentication:

Public-key cryptography supports passwordless solutions such as FIDO2, which is highly secure against phishing and credential attacks. Public keys are stored on the system of the user, hence it is more secure.

Adaptive/Risk-Based Authentication (RBA):

RBA mechanisms evaluate threats and react based on the sophistication of the risk engine and the information employed for proactive defense.

4.2 Usability

Password Authentication:

It is a well-liked choice that irks users with its strict password requirements, constant changes, and difficult recovery.

MFA:

MFA can be clumsy since you have to carry around an extra device or app. However, smartphone push notifications can make a lot of difference.

Single Sign-On (SSO):

SSO enhances user experience with fewer login requests. Users have a better experience with a single login for multiple services.

This technique accelerates login, allowing for instant identity authentication with familiar devices. Password removal streamlines and enhances the user experience.

Adaptive/Risk-Based Authentication (RBA):

RBA intends to be transparent in standard access with additional steps being done only where necessary. This is a balance between providing an unbroken user experience in low-risk scenarios and strong security in high-risk scenarios.

4.3 Performance

Password Authentication:

Performance is quick, typically a single hash comparison on the server.

MFA: A secondary verification process is slower but is feasible for the majority of users.

Single Sign-On (SSO):

SSO is efficient after the first time authentication. Token-based access eliminates the requirement of continuous logging in and speeds up the process.

Passwordless authentication is quick and efficient. Rapid crypto operations and no password typing reduce time.

Adaptive/Risk-Based Authentication (RBA):

RBA can produce slight slowdowns, but these are not substantial for extra security.

4.4 Scalability

Authentication methods scale to handle many concurrent users. SSO and RBA do entail good central management to handle large volumes of users and services.

4.5 Implementation Cost Password Authentication:

It is most economical because it needs minimal infrastructure to hash and store passwords. MFA: Costs are midrange—software MFA is low-cost, but SMS and hardware tokens are high-cost. Single Sign-On (SSO): Implementation is expensive because configuring a centralized identity provider and federating services is complex. Passwordless Authentication: It will cost more to implement in the short term with compatible hardware and software, but maintenance costs are typically less, particularly for eliminating password support. Adaptive/Risk-Based Authentication (RBA): RBA systems are not cheap and need significant investment in machine learning, advanced analysis, and real-time data processing infrastructure.

Technique	Security	Usability	Performance	Scalability	Cost
Password-Based	Low	Medium	High	High	Low
Multi-Factor (MFA)	High	Medium	Medium	High	Medium
Single Sign-On (SSO)	High*	Very High	High	High	High
Passwordless	Very High	Very High	High	High	Medium
Adaptive/Risk-Based	High	High	Medium	High	High

CONCLUSION

The move to cloud computing has transformed the way organizations verify users and ensure security. This submission proves that the conventional password mechanism is not enough to secure vital information in the cloud because of evolving cyber-attacks.

Multi-Factor Authentication (MFA) adds security but triggers implementation and usage issues. Passwordless authentication on the FIDO2 standard and adaptive authentication are future prospects. They offer high security with improved user experience and efficiency, addressing some of the most important cloud security issues.

Core areas of future research include adaptive authentication systems, which require machine learning breakthroughs to minimize false positives. Moreover, passwordless scenarios will need additional research on migration plans and infrastructure integration. Lastly, as quantum computing is in the future, authentication systems will need to be designed to be quantum-resistant to provide cloud service security.

Innovation in such domains is essential to a secure and accessible cloud services future.

REFERENCES

1. Balfanz, D., et al. "A security analysis of the FIDO2 protocol." In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020.
2. Chougrad, H., Zouaki, H., & Alheyane, O. "Deep Convolutional Neural Networks for Breast Cancer Screening." *Computer Methods and Programs in Biomedicine*, 2018.
3. Kabir, H. M. D., et al. "Non-linear Down-Sampling and Signal Reconstruction, Without Folding." 2010 IEEE International Conference on Electronic Measurement & Instruments, 2010.
4. Kumar, S., et al. "A survey on multi-factor authentication for cloud infrastructure." *Journal of Information Security*, 2018.
5. Lundervold, A. S., & Lundervold, A. "An Overview of Deep Learning in Medical Imaging Focusing on MRI." *Zeitschrift für Medizinische Physik*, 2019.

6. Mahajan, P., et al. "A Survey on Adaptive Multi-factor Authentication." *International Conference on Information and Communication Technology for Development*, 2021.
7. Sun, J., et al. "Security analysis of SSO protocols." *Journal of Computer Security*, 2019.
8. Yadav, S. S., & Jadhav, S. M. "Deep Convolutional Neural Network Based Medical Image Classification for Disease Diagnosis." *Journal of Big Data*, 2019.
9. Zhou, X., et al. "A New Deep Convolutional Neural Network Model for Automated Breast Cancer Detection." 2020 International Conference on Big Data and Artificial Intelligence, 2020.
10. Valvano, G., et al. "Convolutional Neural Networks for the Segmentation of Microcalcification in Mammography Imaging." *Journal of Healthcare Engineering*, 2019.