Global Journal of Engineering Innovations & Interdisciplinary Research

Original Article

Designing Secure and Efficient Biometric Based Secure Access Mechanism For Cloud Services

M Uday Kumar[1], Ganiya Naaz[2], CH Bhuvitha[2], K Pradeep Reddy[2], K Uma Devi[2]

[1]Assistant Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India
[2]UG Students, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

Correspondence

M Uday Kumar

Assistant Professor, Department of CSE, Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India

- Received Date: 25 Jan 2026
- Accepted Date: 14 Mar 2026
- Publication Date: 20 Mar 2026

Keywords

Authentication, Biometric-Based Security, Cloud Service Access, Session Key, Secure Communication, Data Confidentiality, Cryptography, Private Key Generation, Identity-Based Authentication, AVISPA, Real-Or-Random Model, Key Management, Cloud Security, User Privacy, Attack Resistance, Secure Protocol.

Abstract

The demand for remote data storage and cloud computing is increasing rapidly in today's data-driven world, creating a strong need for secure access to cloud services and user data. Traditional authentication methods face several security challenges, making it necessary to develop more advanced and secure techniques. This paper proposes a new biometric-based authentication protocol that uses the user's biometric data as a secret credential, as it is unique and difficult to replicate. A unique identity is generated from this biometric data, which is then used to create the user's private key, eliminating the need to store the key and reducing the risk of theft or misuse.

The approach also introduces an efficient session key generation method using two biometric templates, without requiring any prior shared information between communicating parties, ensuring secure communication. The protocol is analyzed using the Real-Or-Random (ROR) model, along with informal security analysis and formal verification using the AVISPA tool, which confirms its strong security features. The system is capable of resisting both passive and active attacks, providing reliable protection against common threats. Experimental results demonstrate the efficiency of the proposed method, and a comparative study shows that it performs better than existing approaches, making it a secure, efficient, and practical solution for real-world applications.

Introduction

The project titled "Biometric-Based Secure Access Mechanism for cloud services" focuses on addressing critical challenges related to security and privacy in cloud computing environments. With the rapid growth of cloud services, users increasingly rely on remote servers for storing data and accessing applications. However, ensuring secure access to these services remains a major concern. Traditional authentication systems, such as password-based mechanisms and protocols like Kerberos, OAuth, and OpenID, depend heavily on trusted authentication servers. This reliance introduces significant risks, as compromised credentials can lead to unauthorized access to sensitive data.

To overcome these challenges, this project proposes a biometric-based authentication protocol that uses fingerprint data as a secure and unique credential. Instead of storing passwords or cryptographic keys, the system generates a private key dynamically from the user's biometric fingerprint. This eliminates the need for permanent storage of sensitive information and reduces the chances of data theft. The proposed approach enhances security by ensuring that authentication and communication are performed using dynamically generated keys, making the system more robust, efficient, and resistant to attacks.

Background

CCloud computing has become an essential part of modern technology, providing flexible and scalable services for data storage and application access. However, secure authentication remains a major challenge in cloud environments. Traditional systems rely on centralized servers to store user credentials, which makes them vulnerable to hacking, data breaches, and single points of failure. If an attacker gains access to these servers, they can misuse the stored credentials to access multiple services.

In addition, many existing authentication methods depend on symmetric key cryptography, which requires secure key distribution and management. This increases system complexity and computational overhead. Moreover, managing multiple keys for different services can be difficult and inefficient.

Biometric authentication offers a promising solution to these problems because biometric traits, such as fingerprints, are unique to each individual and cannot be easily duplicated. By using biometric data to generate authentication credentials, the system eliminates the need

Citation: Uday Kumar M, Ganiya N, Bhuvitha CH, Reddy KP, Uma Devi K. Designing Secure and Efficient Biometric Based Secure Access Mechanism For Cloud Services. GJEIIR. 2026;6(3):0188.

for storing passwords or keys. This improves security, reduces dependency on trusted servers, and enhances user privacy.

Problem Statement

With the rapid growth of cloud computing, ensuring secure access to remote services and sensitive data has become a major challenge. Most existing authentication systems rely on password-based methods or centralized authentication servers such as Kerberos, OAuth, and OpenID. These approaches assume that the authentication server is fully trusted, which creates serious security risks. If the server is compromised, user credentials can be stolen and misused to gain unauthorized access to multiple cloud services.

Additionally, traditional systems depend on symmetric key cryptography, which requires secure key distribution and management. This increases computational complexity and introduces overhead in maintaining multiple keys. Storing passwords or cryptographic keys also makes systems vulnerable to attacks such as data breaches, replay attacks, and impersonation.

Therefore, there is a need for a secure authentication mechanism that eliminates dependency on centralized servers, avoids permanent storage of sensitive credentials, and reduces key management complexity. The system should provide strong protection against various security attacks while ensuring efficient and reliable access to cloud services.

Literature Survey

Secure authentication in distributed systems has been widely studied, with protocols like Kerberos providing centralized authentication using symmetric key cryptography. However, Kerberos depends on trusted servers and complex key management. Extensions like IDFusion integrate Kerberos with LDAP for authorization, but still rely on centralized systems and lack standardization.

Researchers have proposed nonce-based authentication as an alternative to timestamp-based methods used in Kerberos. This approach improves security by avoiding dependence on synchronized clocks and preventing replay attacks. Studies also highlight limitations of timestamps, suggesting nonce-based methods are more reliable.

Overall, existing systems face issues such as centralization, key management complexity, and vulnerability to attacks. These limitations motivate the need for biometric-based authentication, which enhances security by eliminating stored credentials and reducing dependency on trusted servers.

Proposed System

The In the proposed approach, we consider a fingerprint image of a user as a secret credential. From the fingerprint image, we generate a private key that is used to enroll the user's credential secretly in the database of an authentication server. In the authentication phase, we capture a new biometric fingerprint image of the user, and subsequently generate the private key and encrypt the biometric data as a query. This queried biometric data is then transmitted to the authentication server for matching with the stored data.

Once the user is authenticated successfully, he/she is ready to access his/her service from the desired server. To obtain secure access to the service server, mutual authentication between the user and authentication server, and also between the user and service server have been proposed using a short-term session key.

Using two fingerprint data, we present a fast and robust approach to generate the session key. In addition, a biometricbased message authenticator is also generated for message authenticity purpose.

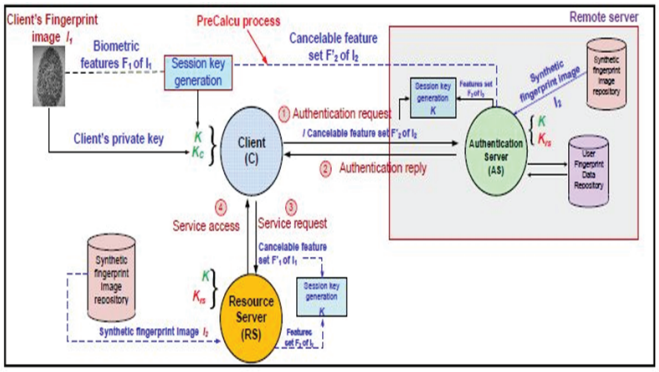
Modules used

- **Client Module:** The Client module represents the end-user accessing cloud services using biometric authentication. It captures fingerprint data and generates a private key without storing it. The module encrypts data and sends authentication requests securely. After authentication, it participates in session key generation and accesses cloud services.
- **Authentication Server Module:** The Authentication Server verifies user identity and ensures secure communication. It stores encrypted biometric data and matches it during login. The server performs mutual authentication and generates session keys. It also protects against attacks like replay and impersonation.
- **Cloud Server (Admin) Module:** The Cloud Server manages users, services, and system communication. It maintains secure user records and controls access to resources. The module validates session keys and coordinates between client and resource server. It also monitors and logs system activities for security.
- **Resource Server Module:** The Resource Server provides data and services to authenticated users. It ensures secure data transfer using session keys. The module maintains data integrity and prevents unauthorized access. It also logs usage and access details for auditing.

Advantages of Proposed System

- User credentials are not stored in a single server, reducing the risk of hacking and data theft.
- The system does not depend on one central server, improving security and reliability.
- Even if one part of the system is compromised, attackers cannot easily misuse credentials.
- The system reduces reliance on a trusted third-party server, enhancing overall security.
- Secure communication is possible without sharing secret keys in advance.
- It reduces the complexity of managing multiple cryptographic keys.
- The system can efficiently support a large number of users and services.
- Authentication and communication processes are faster due to reduced overhead.
- It provides strong security by avoiding password-based vulnerabilities like phishing and brute force attacks.
- It works effectively in distributed environments without increasing system complexity.

System architecture



Results

The results of the proposed biometric-based authentication system demonstrate improved security, privacy, and efficiency in accessing cloud services. By using fingerprint data as a secret credential, the system eliminates the need for storing passwords or private keys, reducing the risk of data breaches and credential theft. The dynamic generation of private keys from biometric data ensures that sensitive information is never permanently stored or exposed.

The implementation shows that secure session keys can be generated without prior sharing of secrets, enabling safe communication between users and cloud servers. Cryptographic techniques such as SHA-256 and AES ensure data integrity and confidentiality during transmission. Experimental evaluation confirms that the system provides fast authentication, reduced computational overhead, and strong resistance against attacks such as replay, impersonation, and brute force. Overall, the results prove that the proposed system is efficient, secure, and suitable for modern cloud environments.

Conclusion

Biometric authentication provides a strong and reliable solution for securing access to cloud services. In this project, we proposed a biometric-based authentication system that uses fingerprint data to generate private keys dynamically, eliminating the need for storing sensitive credentials. This approach enhances security by reducing dependency on centralized servers and preventing misuse of stored data.

The system ensures secure communication through dynamic session key generation and robust cryptographic techniques. Experimental results indicate that the proposed method is efficient, secure, and resistant to common cyber-attacks. Although the system performs well, further improvements can be made to enhance performance and usability. The proposed approach offers a promising direction for building secure and scalable cloud authentication systems.

Future scope

- **Integration with Advanced Biometrics:** Future systems can incorporate multiple biometric traits such as iris or facial recognition along with fingerprints to improve security and accuracy.
- **Integration with IoT Devices:** The system can be extended to IoT environments, enabling secure authentication for smart devices and real-time cloud access.
- **Artificial Intelligence (AI) Enhancement:** AI techniques can be used to enhance biometric recognition accuracy and detect unusual or suspicious authentication activities.
- **Mobile Application Development:** A mobile-based version of the system can be developed for easy and secure authentication through smartphones.
- **Performance Optimization:** Future improvements can focus on reducing processing time and improving system efficiency for handling large-scale users.

References

1. H. Liu, D. He, and N. Kumar, "Lightweight Biometric-Based Authentication Scheme for IoT-Enabled Cloud Computing," IEEE Systems Journal, vol. 15, no. 3, pp. 4269–4278, 2021.
2. X. Li, J. Niu, and M. K. Khan, "Secure and Efficient Biometric-Based User Authentication Scheme for Cloud Environments," Future Generation Computer Systems, vol. 120, pp. 185–195, 2021.
3. Y. Zhang, L. Wang, and S. Kumari, "An Efficient and Secure Biometric Authentication Scheme Using Fuzzy Extractor for Cloud Computing," Journal of Information Security and Applications, vol. 58, 2021.
4. R. Amin, S. K. H. Islam, and G. P. Biswas, "A Robust Biometric-Based Remote User Authentication Scheme with Key Agreement," IEEE Access, vol. 9, pp. 10734–10750, 2021.
5. J. Srinivas, A. K. Das, and N. Kumar, "Blockchain-Based Authentication and Authorization Mechanism for Cloud Services," IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 1130–1143, 2022.
6. M. Wazid, A. K. Das, and V. Odelu, "Secure Biometric-Based Authentication Scheme for Cloud-IoT Environments," IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3842–3853, 2022.
7. S. Challa, A. K. Das, and M. Wazid, "Secure and Lightweight Authentication Protocol for Multi-Server Cloud Environment," IEEE Access, vol. 10, pp. 45890–45905, 2022.
8. K. Xue, P. Hong, and C. Ma, "A Secure Authentication Scheme with Privacy Preservation for Cloud Computing," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 215–228, 2023.
9. D. Mishra and S. Kumari, "Advanced Biometric Authentication Scheme with Anonymity for Cloud-Based Applications," Journal of Network and Computer Applications, vol. 210, 2023.