ENHANCED SECURITY IN MOBILE-EDGE COMPUTING USING BIOMETRIC AUTHENTICATION

GUIDE : P.RAMYA M.Tech(CSE)
Assistant Professor, Department of CSE-AI&DS
Eluru College of Engineering and Technology

TEAM LEAD : P. ROHITH SANTHOSH[1]
TEAM MEMBERS: D. PAVAN KALYAN[2]
V. HARI KARTHIK[3]
S. RAKSHITHA [4]

Eluru College of Engineering and Technology

ABSTRACT

With the era of fast-paced technology development, authenticating securely and efficiently in Mobile-Edge Computing (MEC) scenarios is imperative. The project introduces a Biometric-Based Anonymous Authentication Scheme that promotes privacy for users and ensures strong security. Conventional authentication schemes usually have security issues and inefficiency, which is not appropriate for resource-limited MEC settings. Our scheme utilizes biometric credentials to support a secure, anonymous, and lightweight authentication protocol. By combining cryptographic methods with optimized computation and communication overhead, the system proposed here minimizes latency while strengthening security. The authentication model is thoroughly tested for security vulnerabilities like replay attacks, man-in-the-middle attacks, and impersonation. Comparison analysis proves our method to efficiently improve performance while keeping security high, thus a good solution for secure MEC authentication.

1. INTRODUCTION

In the contemporary digital age, the fast growth of cloud computing and edge computing has created a growing need for secure and effective authentication mechanisms. Mobile-Edge Computing (MEC) is a strong paradigm that brings cloud-like services closer to the end-users, mitigating latency and enhancing computational efficiency. Nevertheless, as MEC networks grow, providing strong security and privacy protection for user authentication is a strong challenge. The traditional methods of authentication like passwords, PINs, and token-based authentication are susceptible to security vulnerabilities like phishing attacks, brute-force attacks, and stolen credentials. To overcome these, biometric authentication has become popular because of its individuality, ease, and high security.

The present project aims to introduce a Secure and Efficient Biometric-Based Anonymous Authentication Scheme for Mobile-Edge Computing to increase authentication security without compromising user privacy. Biometric authentication, involving fingerprint scanning, face recognition, and iris detection, provides a secure and un-replicable form of user authentication. Biometric data storage and transmission raise data privacy and security threat concerns. To overcome such risks, the authentication scheme being proposed combines biometric authentication with cryptographic mechanisms for safe transmission and storage of the user credentials with anonymity preserved. Requirement of Secure Authentication in MEC Mobile-Edge Computing is extensively used across different industries, such as healthcare, finance, and smart cities, where security and privacy of data take precedence. MEC facilitates real-time processing and minimizes reliance on centralized cloud infrastructure but, in the process, also raises security concerns, including unauthorized access, identity spoofing, and data leakage. Traditional authentication mechanisms tend to neglect these issues because of high computational complexity and vulnerability to cyber-attacks. The performance of the scheme is compared with existing authentication methods to demonstrate its superiority in terms of security, efficiency, and scalability. The results show that our approach significantly reduces authentication overhead while maintaining a high level of security, making it an ideal solution for Mobile-Edge Computing environments.

2. EXISTING SYSTEM

The existing authentication systems for Mobile-Edge Computing (MEC) primarily rely on traditional methods such as password-based authentication, One-Time Passwords (OTP), and multi-factor authentication (MFA). These methods provide a basic level of security but suffer from several vulnerabilities. Passwords are susceptible to brute-force attacks, phishing, and credential leaks. OTP-based authentication, while more secure, is often inconvenient due to dependency on mobile networks and user input errors. Multi-factor authentication adds security layers but increases authentication complexity and user friction.

DISADVANTAGES OF EXISTING SYSTEM

- Security Vulnerabilities: Traditional authentication methods are prone to hacking, phishing, and credential leaks.
- Privacy Concerns: Centralized storage of biometric data poses a risk of identity theft if breached.
- Lack of Anonymity: Existing systems fail to provide complete user anonymity, making users susceptible to tracking and profiling.

3. PROPOSED SYSTEM

The suggested system presents a Secure and Efficient Biometric-Based Anonymous Authentication Scheme for Mobile-Edge Computing (MEC). The system incorporates biometric authentication together with light-weight cryptographic mechanisms to provide security, privacy, and efficiency. We use LBPH Algorithm. The Local Binary Patterns Histogram (LBPH) algorithm is a powerful and widely used face recognition technique in computer vision.

Rather than depending on conventional passwords or centralized biometric databases, the suggested system employs privacy-preserving biometric authentication, allowing users to stay anonymous during identity verification securely. Advanced security measures like Elliptic Curve Cryptography (ECC) and Zero-Knowledge Proofs (ZKP) are used to avoid unauthorized access and biometric data compromises. The system also includes multi-modal biometrics to enhance the accuracy of authentication and resistance against spoofing attacks.

ADVANTAGES PROPOSED SYSTEM

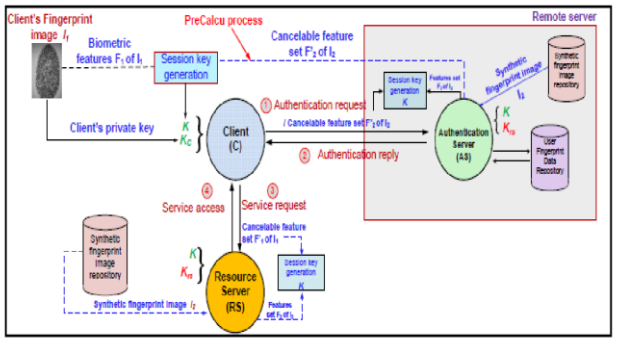
- Preservation of Privacy: Supports anonymous authentication without tracking identities or making them subject to profiling.
- Less Computational Overhead: Deploys lightweight cryptographic schemes to ensure speedy authentication within MEC scenarios.
- Multi-Modal Biometrics: Leverages multiple biometric features to achieve greater accuracy and attack resistance.

4. SYSTEM ARCHITECTURE

The system architecture for Enhanced Security in Mobile-Edge Computing Using Biometric Authentication is designed to provide a secure and efficient authentication mechanism in edge computing environments. The architecture consists of multiple layers, including the user authentication layer, edge computing layer, and cloud storage layer. At the user authentication layer, biometric data such as fingerprints, facial recognition, or iris scans are collected and securely transmitted for verification. The edge computing layer processes authentication requests locally, reducing latency and improving response times compared to traditional cloud-based authentication. This layer also employs encryption and machine learning techniques to enhance security and detect anomalies.

The cloud storage layer ensures secure backup and retrieval of biometric templates, enabling seamless user access across different edge nodes. The system integrates real-time authentication, access control mechanisms, and secure communication channels to protect against cyber threats. By leveraging biometric authentication in mobile-edge computing, this architecture enhances security while maintaining high performance and scalability.

This layer supports seamless authentication across multiple edge nodes and integrates secure backup mechanisms to prevent data loss or tampering. Additionally, the Security and Access Control Mechanism enhances protection by incorporating multi-factor authentication, secure key management, and intrusion detection systems. Blockchain technology or distributed ledger systems can also be integrated to improve data integrity and prevent unauthorized modifications.



5. REFERENCES

[1] C. Neuman, S. Hartman, K. Raeburn, "The kerberos network authentication service (v5)," RFC 4120, 2005.
[2] "OAuth Protocol." [Online]. Available: http://www.oauth.net/
[3] "OpenID Protocol." [Online]. Available: http://openid.net/
[4] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.
[5] A. Kehne, J. Schonwalder, and H. Langendorfer, "A nonce-based protocol for multiple authentications," ACM SIGOPS Operating System Review, vol. 26, no. 4, pp. 84–89, 1992.
[6] B. Neuman and S. Stubblebine, "A note on the use of timestamps as nonces," Oper. Syst. Rev., vol. 27, no. 2, pp. 10–14, 1993.
[7] J. Astorga, E. Jacob, M. Huarte, and M. Higuero, "Ladon : endto-end authorisation support for resource-deprived environments," IET Infomration Security, vol. 6, no. 2, pp. 93–101, 2012.
[8] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," Washington D.C., USA, October 2003, pp. 62–72.
[9] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, and D. Culler, "SPINS: security protocols for sensor networks," ACM Wireless Networking, vol. 8, no. 5, pp. 521–534, 2002.
[10] P. Kaijser, T. Parker, and D. Pinkas, "SESAME: The solution to security for open distributed systems," Computer Communications, vol. 17, no. 7, pp. 501–518, 1994.
[11] G. Wettstein, J. Grosen, and E. Rodriguez, "IDFusion: An open architecture for Kerberos based authorization," Proc. AFS and Kerberos Best Practices Workshop, June 2006.
[12] M. Walla, "Kerberos explained," Windows 2000 Advantage Magazine, 2000. [13] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1070–1081, 2015. [14] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An efficient biometric authentication protocol for wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 2013, pp. 1–13, 2013, Article ID 407971, http://dx.doi.org/ 10.1155/2013/407971. [15] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 316 – 323, 2013.
[16] M. Turkanovic, B. Brumen, and M. Holbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion," Ad Hoc Networks, vol. 20, pp. 96 – 112, 2014. [17] M. Park, H. Kim, and S. Lee, "Privacy Preserving Biometric-Based User Authentication Protocol Using Smart Cards," in 17th International Conference on Computational Science and Engineering, Chengdu, China, 2014, pp. 1541–1544. [18] P. K. Dhillon and S. Kalra, "A lightweight biometrics based remote user authentication scheme for IoT services," Journal of Information Security and Applications, vol. 34, pp. 255 – 270, 2017.
[19] S. D. Kaul and A. K. Awasthi, "Security Enhancement of an Improved Remote User Authentication Scheme with Key Agreement," Wireless Personal Communications, vol. 89, no. 2, pp. 621–637, 2016.
[20] D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient and Secure Biometric-Based User Authenticated Key Agreement Scheme with Anonymity," Security and Communication Networks, vol. 2018, pp. 1–14, 2018, Article ID 9046064, https://doi.org/10.1155/2018/9046064.
[21] D. Dolev and A. C. Yao, "On the security of public key protocols," IEEE Transactions on Information Theory, vol. 29, no. 2, pp. 198–208, 1983.
[22] A. K. Das, "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 9, no. 1, pp. 223–244, 2016.
[23] "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," International Journal of Communication Systems, vol. 30, no. 1, pp. 1–25, 2017.
[24] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credentialbased security scheme with mutual authentication and key agreement for wireless sensor networks," Sensors, vol. 13, no. 8, pp. 9589–9603, 2013.
[25] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credentialbased mutual authentication and key agreement scheme for wireless sensor networks," in International Symposium on Wireless and pervasive Computing (ISWPC), Taipei, Taiwan, 2013, pp. 1–6.
[26] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," ELEKTRONIKA IR ELEKTROTECHNIKA, vol. 19, no. 6, pp. 109 – 116, 2013. [27] R. Amin and G. P. Biswas,

AUTHOR'S PICS

GUIDE - P. RAMYA M.Tech(CSE) Working as Assistant Professor in Department of CSE-(AI&DS), Eluru College Of Engineering And Technology, Eluru.

EMAIL - ramyaparasa99@gmail.com

TEAM LEAD - P. ROHITH SANTHOSH B.Tech in Department of CSE-(AI&DS), Eluru College Of Engineering And Technology, Eluru.
EMAIL – rohithsanthosh769@gmail.com

TEAM MEMBER – D. PAVAN KALYAN
B.Tech in Department of CSE-(AI&DS), Eluru College Of Engineering And Technology, Eluru.

EMAIL - kalyannaidudantu@gmail.com

TEAM MEMBER – V. HARI KARTHIK
B. Tech in Department of CSE-(AI&DS), Eluru College Of Engineering And Technology, Eluru.

EMAIL – no.9391747610@gmail.com

TEAM MEMBER – S. RAKSHITHA B. Tech in Department of CSE-(AI&DS), Eluru College Of Engineering And Technology, Eluru.

EMAIL – saidamrakshitha@gmail.com