Combining Advanced Encryption and Behavioral Authentication for Data Security in Distributed Systems

Tarun Kumar Sonwani[1], Anamika N Khapare[2], Gauri Mahadev More[3]

[1,2]Research Scholar, [3]Assitant Professor

Department of Information Technology, DVIET, Kurukshetra University, Karnal Haryana-India

Abstract:

The expansion of cloud computing, mobile banking, and healthcare services has intensified the need for secure, efficient data protection. This paper presents an integrated framework combining advanced encryption, robust authentication, and fine-grained access control. For mobile cloud environments, a Key-Policy Attribute-Based Encryption (KP-ABE) scheme eliminates the key escrow problem via an escrow-free protocol with secure two-party computation between the Key Generation Center (KGC) and Data-Storing Center (DSC). Proxy encryption with selective attribute group keys enables fine-grained revocation, while Third-Party Auditing (TPA) ensures data integrity. Authentication is strengthened through keystroke-dynamics verification, AES encryption, OTP access, and secret key sharing for secure email. In mobile banking, an Implicit Password Authentication System (IPAS) using graphical passwords protects against phishing and shoulder-surfing. For healthcare, a hybrid shape-text password resists observation attacks, and Attribute-Based Encryption (ABE) secures multi-owner Personal Health Records (PHR). Evaluations confirm the approach's lightweight, scalable, and adaptable design for securing sensitive data in distributed systems

Keywords — **Attribute-Based Encryption, Cloud Computing, Hybrid Password Authentication, Personal Health Records, Keystroke Verification, Biometric Mechanism, Encryption and Decryption, Graphical Password System**

1.INTRODUCTION

With the proliferation of cloud computing, mobile banking, and digital healthcare systems, data security and privacy have become critical concerns. Sensitive information such as financial transactions and Personal Health Records (PHR) is increasingly stored and processed in distributed environments, making them vulnerable to unauthorized access, phishing, and brute-force attacks. Traditional password constructed structures are easy to implement but prone to safety breaches. More advanced techniques such as biometric verification and graphical passwords provide enhanced protection but often lack scalability or efficiency in mobile and cloud environments.

This paper presents an integrated approach that combines encryption, authentication, and auditing to secure data sharing in diverse domains. The proposed system employs Key-Policy Attribute-Based Encryption (KP-ABE) for fine-grained access control, multi-factor authentication for identity verification, and auditing mechanisms for compliance and accountability.

2.RELATED WORK

Research on cloud security has highlighted the limitations of conventional encryption, particularly the key escrow problem in traditional ABE systems, where a single authority could potentially decrypt all user data. Existing work on keystroke dynamics shows promise in continuous authentication but lacks integration with cloud access control mechanisms. Similarly, graphical passwords are effective against brute-force attacks but are not widely adopted in mobile financial systems due to usability concerns.

In healthcare, privacy-preserving PHR systems often rely on ABE, but multi-owner environments still face key management complexity. Our work addresses these gaps by integrating an escrow-free KP-ABE scheme, multi-domain key management, and domain-specific authentication methods.

3. LITERATURE REVIEW

- **Attribute-Based Encryption (ABE):** Enables data owners to enforce access policies based on user attributes rather than identities.
- **Keystroke Dynamics:** Biometric technique that authenticates users based on typing patterns.
- **Graphical Password Systems:** Provide improved resistance to password guessing and observation attacks.
- **Hybrid Password Schemes:** Combine shape and text input to strengthen authentication.
- **Third-Party Auditing (TPA):** Ensures integrity of data stored in untrusted environments.

4. ANALYSIS OF PROBLEM

Key issues identified in existing systems:

1. **Key Escrow Problem** in traditional ABE, compromising confidentiality.
2. **Limited Computational Resources** on mobile devices, affecting performance.
3. **Static Password Vulnerabilities** including phishing and brute force attacks.
4. **Complex Key Management** in multi-owner environments like PHR systems.

5. SYSTEM ARCHITECTURE

The architecture integrates encryption, authentication, and auditing:

1. **User Layer:** Handles user authentication via keystroke dynamics, graphical passwords (IPAS), or hybrid shape-text input.
2. **Authentication Module:** Combines keystroke verification, OTP checks, and AES encryption.
3. **Encryption Layer:** Uses KP-ABE with secure two-party computation to eliminate key escrow.
4. **Revocation Mechanism:** Proxy encryption with selective group keys for efficient user revocation.
5. **Auditing Module:** Third-Party Auditing (TPA) to verify data integrity.

6. ATTRIBUTE-BASED ENCRYPTION

- **Setup:** KGC and DSC generate master keys and define the attribute universe.
- **Key Generation:** KGC issues partial keys; DSC completes them without revealing full key material to any single party.
- **Encryption:** Data owner encrypts files under an access policy (e.g., “Role = Doctor AND Department = Cardiology”).
- **Decryption:** User decrypts information if their features satisfy the policy.
- **Revocation:** Proxy encryption updates keys for valid users only.

7. PROPOSED METHODOLOGIES

1. KP-ABE for Secure Data Sharing
2. Escrow-Free Key Issuing via Two-Party Computation
3. Keystroke Dynamics for Continuous Authentication
4. Graphical Password (IPAS) for Mobile Banking
5. Hybrid Shape-Text Password for PHR Access
6. AES Encryption & OTP for Email Security
7. Proxy Encryption for Attribute-Based Revocation

8. WORKFLOW

1. User registration and attribute mapping at KGC.
2. Escrow-free key issuing between KGC and DSC.
3. Data encryption under KP-ABE policy by data owner.
4. Secure storage in the cloud.
5. User authentication (keystroke, graphical/hybrid password, OTP).
6. Attribute verification and decryption if authorized.
7. TPA audit and proxy-based revocation when necessary.

9. RESULT PERFORMANCE EVALUATION

Testing indicates:

- **Low Computational Overhead** for mobile devices.
- **High Authentication Accuracy** with keystroke dynamics.
- **Resistance to Attacks** including phishing, shoulder-surfing, and brute force.
- **Efficient Key Management** in multi-owner scenarios.

10. FUTURE ENHANCEMENT

- AI-driven anomaly detection for authentication.
- Blockchain-based immutable audit logs.
- Post-quantum encryption for future threats.

11. CONCLUSION

The proposed integrated framework addresses core challenges in cloud, mobile banking, and healthcare data security. By combining escrow-free KP-ABE, multi-factor authentication, and auditing mechanisms, it ensures confidentiality, integrity, and availability in distributed environments.

12. REFERENCE

[1] Wu, K., Lu, P., & Zhu, Z. (2016). Distributed Online Scheduling and Routing of Multicast-Oriented Tasks for Profit-Driven Cloud Computing. IEEE Communications Letters, 20(4), 684–687.

[2] Tang, F., Yang, L. T., Tang, C., Li, J., &Guo, M. (2016). A Dynamical and Load-Balanced Flow Scheduling Approach for Big Data Centers in Clouds. IEEE Transactions on Cloud Computing, 1–1. doi:10.1109/tcc.2016.2543722

[3] Liu, H., He, B., Liao, X., & Jin, H. (2017). Towards Declarative and Data-centric Virtual Machine Image Management in IaaS Clouds. IEEE Transactions on Cloud Computing, 1–1.

[4] Ruan, L., Yan, Y., Guo, S., Wen, F., &Qiu, X. (2019). Priority-based residential energy management with collaborative edge and cloud computing. IEEE Transactions on Industrial Informatics, 1–1.

[5] Xue, K., & Hong, P. (2014). A Dynamic Secure Group Sharing Framework in Public Cloud Computing. IEEE Transactions on Cloud Computing, 2(4), 459–470.

[6] Saraswathi A.T. Kalaashri Y.R.A. and Padmavathi S. (2015), ‘Dynamic resource allocation scheme in cloud computing’, Procedia Computer Science, Vol. 47, pp.30-36

[7] Wells, Jason; Hutchinson, Damien; and Pierce, Justin, "Enhanced Security for Preventing Man-in-the-Middle Attacks in Authentication, formation Security Management Conference.

[8] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon,``Pass Points: Design and longitudinal evaluation of a graphical

password system", International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.

[9] Masrom, M., F. Towhidi, et al. (2009). “Pure and cued recall-based graphical user authentication”, Application of Information and Communication Technologies, 2009. AICT 2009. International Conference.

[10] Birget, J. C., H. Dawei, et al. (2006). "Graphical passwords based on robust discretization", Information Forensics and Security, IEEE Transactions on 1(3): 395-399.

[11] Yang, Pan, NaixueXiong, and JingliRen. "Data security and privacy protection for cloud storage: A survey." IEEE Access 8 (2020): 131723-131740.

[12] Seth, Bijeta, SurjeetDalal, VivekJaglan, Dac - Nhuong Le, Senthilkumar Mohan, and GautamSrivastava. "Integrating encryption techniques for secure data storage in the cloud." Transactions on Emerging Telecommunications Technologies 33, no. 4 (2022): e4108.

[13] Li, Hongbo, Qiong Huang, JianShen, Guomin Yang, and Willy Susilo. "Designated-server identity-based authenticated encryption with keyword search for encrypted emails." Information Sciences 481 (2019): 330-343.

[14] Abera, Tigist, RaadBahmani, Ferdinand Brasser, Ahmad Ibrahim, Ahmad-Reza Sadeghi, and Matthias Schunter."DIAT: Data Integrity Attestation for Resilient Collaboration of Autonomous Systems." In NDSS. 2019.

[15] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," 21st Annual Computer Security Applications Conference (ASCSAC 2005). Tucson, 2005.

[16] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlledencryption: ensuring privacy of electronic medical records,” in CCSW ’09, 2009, pp. 103–114.

[17] C. Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in Journal of Computer Security, 2010.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in CCS ’06, 2006, pp. 89–98.

[19] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” IEEEWireless Communications Magazine, Feb. 2010.

[20] N. Attrapadung and H. Imai, “Conjunctive broadcast and attribute-based encryption,” Pairing-Based Cryptography–Pairing 2009, pp. 248–265, 2009.