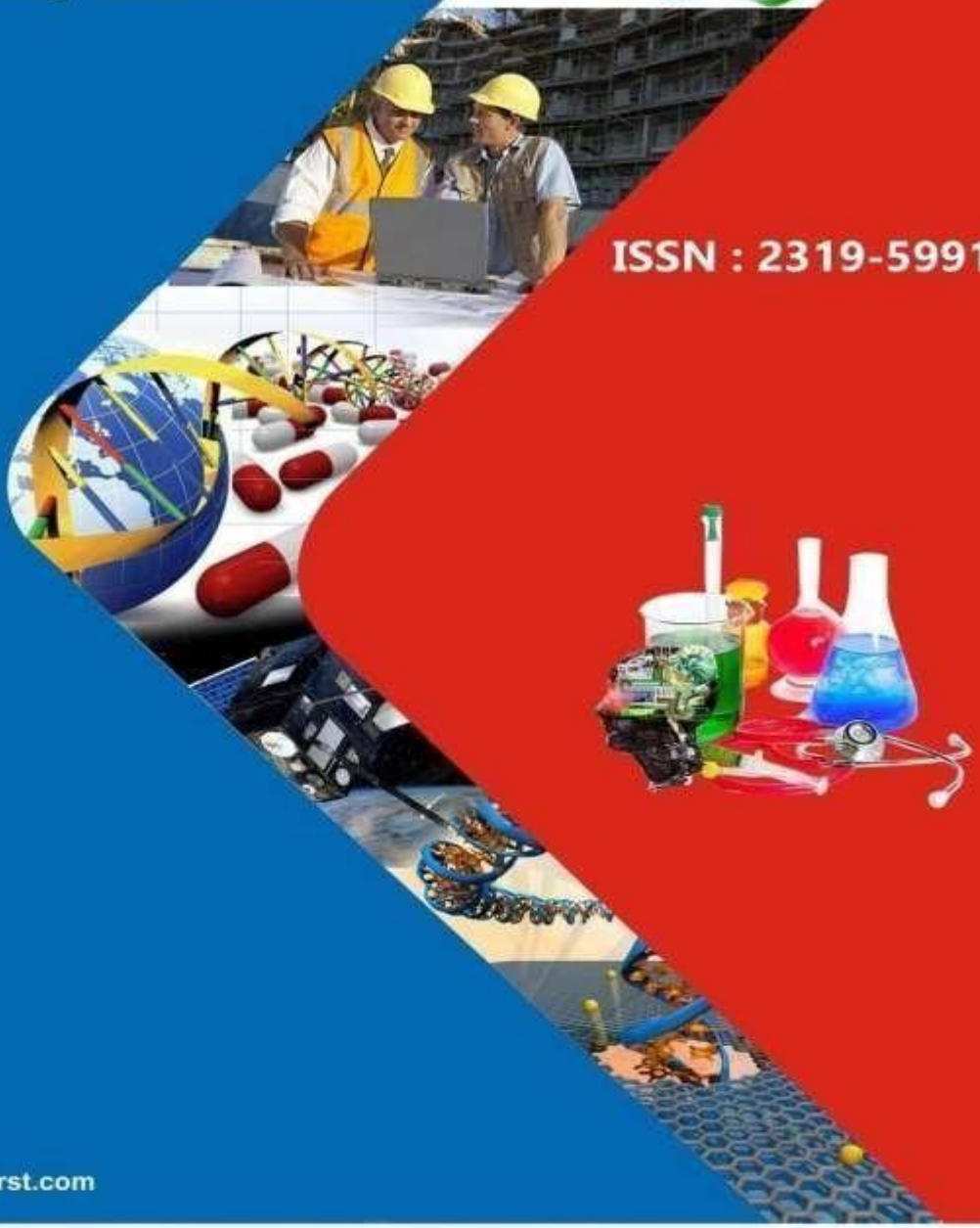
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

Revocable Attribute-based Data Storage in Mobile Clouds

Y.SRINIVASA RAJU, Associate professor,
Department of MCA
srinivasaraju.y@gmail.com
B V Raju College, Bhimavaram

kairam venkateswara Rao (2285351046)
Department of MCA
venkateshkairam956@gmail.com
B V Raju College, Bhimavaram

ABSTRACT

The Java project on "Revocable Attribute-based Data Storage in Mobile Clouds" focuses on enhancing the security and privacy of data stored in mobile cloud environments through revocable attribute-based access control mechanisms. In this project, the aim is to develop a secure and efficient data storage system that allows users to specify fine-grained access policies based on attributes such as user roles, data sensitivity levels, and contextual information. The system leverages attribute-based encryption (ABE) techniques to encrypt data with access policies embedded in ciphertext, enabling flexible and scalable access control enforcement. Additionally, the project integrates revocation mechanisms to enable dynamic updates of access privileges, ensuring that revoked users or compromised devices are promptly removed from the system's access control lists. The implementation utilizes Java programming language for building the backend infrastructure, cryptographic primitives, and access control logic. Key components of the project include the development of encryption and decryption modules, access policy management interfaces, and revocation management mechanisms. Through this project, the goal is to provide mobile cloud users with robust data protection mechanisms that mitigate the risk of unauthorized access, data leakage, and privacy breaches while maintaining scalability, efficiency, and usability in resource-constrained environments.

INTRODUCTION

This paper addresses the critical need for enhancing the security and privacy of data stored in mobile cloud environments. As mobile devices become increasingly ubiquitous and integral to our daily lives, the need for secure and efficient data storage solutions in mobile clouds has become more pressing. This project aims to tackle this challenge by developing a data storage system that employs revocable attribute-based access control mechanisms, ensuring that data remains secure and accessible only to authorized users. At the heart of this project lies the concept of attribute-based encryption (ABE), a powerful cryptographic technique that enables fine-grained access control over encrypted data. ABE allows data owners to specify access policies based on various attributes, such as user roles, data sensitivity levels, and contextual information. These access policies are embedded directly into the ciphertext, ensuring that only users whose attributes satisfy the policy can decrypt and access the data. This approach provides a high level of flexibility and scalability, making it well-suited for dynamic and heterogeneous mobile cloud environments.

One of the primary objectives of this project is to integrate revocation mechanisms into the ABE framework. In any secure data storage system, it is essential to have the ability to revoke

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

access privileges when necessary, such as when a user leaves an organization or when a device is compromised. The revocation mechanisms developed in this project enable dynamic updates of access control lists, ensuring that revoked users or compromised devices are promptly removed from the system. This feature is crucial for maintaining the integrity and security of the data stored in mobile clouds. The implementation of this project involves the development of several key components using the Java programming language. The backend infrastructure forms the core of the system, handling data storage, encryption, and decryption processes. Cryptographic primitives are employed to ensure the robustness and security of the encryption algorithms used. Additionally, access control logic is implemented to enforce the specified access policies and manage user attributes effectively.

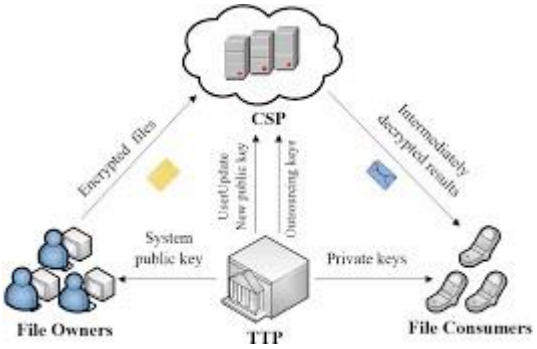


Fig 1. Proposed system architecture

A significant aspect of this project is the development of encryption and decryption modules. These modules are responsible for encrypting data with the specified access policies and decrypting data based on the attributes of the requesting user. The encryption module takes data and an access policy as input, producing ciphertext that can only be decrypted by users whose attributes satisfy the policy. The decryption module, on the other hand, verifies the user's attributes against the policy embedded in the ciphertext and decrypts the data if the attributes match. Access policy management interfaces are another crucial component of this project. These interfaces allow data owners to define and manage access policies easily. Users can specify complex access policies using a combination of attributes, enabling a high degree of customization and control over who can access the data. The interfaces are designed to be user-friendly, ensuring that even users with limited technical knowledge can effectively manage their data access policies.

Revocation management mechanisms are also developed to support the dynamic nature of access control in mobile clouds. These mechanisms allow data owners to revoke access privileges for specific users or devices without disrupting the overall system. When a user or device is revoked, the system updates the access control lists and ensures that the revoked entities can no longer access the encrypted data. This functionality is essential for maintaining the security of the system in the face of changing user roles and potential security threats. The primary goal of this project is to provide mobile cloud users with robust data protection

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

mechanisms that mitigate the risk of unauthorized access, data leakage, and privacy breaches. By leveraging ABE techniques and integrating revocation mechanisms, the project aims to offer a secure and efficient data storage solution that is both scalable and usable in resource-constrained mobile environments. The system is designed to handle the unique challenges posed by mobile cloud environments, such as limited computational resources, intermittent connectivity, and diverse user requirements. In conclusion, the "Revocable Attribute-based Data Storage in Mobile Clouds" project represents a significant advancement in the field of secure data storage for mobile cloud environments. By combining the strengths of attribute-based encryption with dynamic revocation mechanisms, the project provides a comprehensive solution to the challenges of data security and privacy in mobile clouds. The implementation of this project using Java ensures a robust and efficient backend infrastructure capable of handling the demands of modern mobile cloud applications. Through this project, users can have greater confidence in the security and privacy of their data, knowing that their access control policies are enforced with precision and flexibility.

LITERATURE SURVEY

The increasing reliance on mobile cloud environments for data storage and access necessitates robust security mechanisms to protect sensitive information. One such mechanism is Attribute-Based Encryption (ABE), which allows fine-grained access control by associating access policies with data. ABE schemes, first introduced by Sahai and Waters, have evolved into various forms such as Key-Policy ABE (KP-ABE) and Ciphertext-Policy ABE (CP-ABE), each catering to different application requirements. KP-ABE allows policies to be embedded in user keys, while CP-ABE embeds policies in the ciphertext, offering flexibility in defining access controls directly by data owners. A significant challenge in ABE systems is the revocation of access rights, which is critical in dynamic environments like mobile clouds. Traditional ABE schemes do not inherently support efficient revocation, leading to potential security risks when users' access rights change or devices are compromised. Several approaches have been proposed to address this issue. One such approach involves combining ABE with proxy re-encryption (PRE), allowing a trusted proxy to re-encrypt data when access policies change. Another method involves time-based attributes, where access rights expire automatically, requiring periodic key updates.

Mobile cloud environments introduce additional complexities due to resource constraints such as limited bandwidth, storage, and processing power. This necessitates lightweight cryptographic operations and efficient key management. Recent research has focused on optimizing ABE schemes for mobile environments. Techniques such as outsourcing heavy computations to the cloud or using hybrid encryption methods, where symmetric encryption is combined with ABE, have shown promise in reducing computational overhead on mobile devices. The integration of revocation mechanisms in ABE has seen several innovative approaches. A notable method is the use of attribute revocation, where specific attributes associated with a user's key can be revoked without affecting other users. This granular revocation is achieved through methods like ciphertext update and key update protocols.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

Ciphertext update protocols involve re-encrypting data with new policies, while key update protocols require updating users' keys without altering the ciphertext. Moreover, the advent of blockchain technology has opened new avenues for secure and transparent access control in mobile clouds. Blockchain can provide an immutable audit trail for access control policies and revocation events, enhancing trust and accountability. Combining ABE with blockchain can offer a decentralized and tamper-proof system for managing access rights and revocations.

Despite these advancements, several challenges remain in implementing ABE with efficient revocation in mobile clouds. These include ensuring minimal performance degradation, maintaining scalability with increasing users and data, and addressing privacy concerns related to the exposure of attribute information. Research is ongoing to develop more robust, scalable, and privacy-preserving ABE schemes suitable for mobile cloud environments. In conclusion, the literature indicates a significant effort towards enhancing ABE schemes with efficient revocation mechanisms tailored for mobile cloud environments. The proposed solutions aim to balance security, efficiency, and usability, addressing the unique challenges posed by resource-constrained mobile devices and the dynamic nature of cloud-based access control.

PROPOSED SYSTEM

The proposed system, "Revocable Attribute-based Data Storage in Mobile Clouds," aims to enhance data security and privacy by implementing a revocable attribute-based access control mechanism. The system leverages Ciphertext-Policy Attribute-Based Encryption (CP-ABE) to enable data owners to define fine-grained access policies directly on the data. These policies are embedded in the ciphertext, ensuring that only users with the appropriate attributes can decrypt and access the data. The system architecture consists of several key components: the encryption and decryption modules, the access policy management interface, and the revocation management mechanism. The encryption module allows data owners to specify access policies based on attributes such as user roles, data sensitivity levels, and contextual information. These policies are then embedded in the ciphertext using CP-ABE, ensuring that data is encrypted in a way that only authorized users can decrypt it.

The decryption module is responsible for verifying user attributes against the access policies embedded in the ciphertext. If a user's attributes satisfy the policy, the module decrypts the data; otherwise, access is denied. This module utilizes efficient cryptographic operations to minimize the computational overhead on mobile devices, ensuring that the decryption process is lightweight and suitable for resource-constrained environments. The access policy management interface provides a user-friendly platform for data owners to define and manage access policies. This interface allows for the creation, modification, and deletion of policies, enabling dynamic and flexible access control. Data owners can specify complex policies involving multiple attributes and logical conditions, providing granular control over data access. Revocation management is a critical component of the proposed system. The revocation mechanism ensures that users or devices that are no longer authorized to access data are promptly removed from the system's access control list. This is achieved through attribute

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

revocation, where specific attributes associated with a user's key can be revoked without affecting other users. The system employs key update protocols, where updated keys are issued to non-revoked users, and ciphertext update protocols, where the ciphertext is re-encrypted with new policies.

The system also integrates with a trusted proxy server to facilitate the revocation process. The proxy server handles the re-encryption of data and the distribution of updated keys, offloading these computationally intensive tasks from the mobile devices. This ensures that the revocation process is efficient and does not degrade the performance of the mobile devices. To address the challenges of resource constraints in mobile environments, the system employs hybrid encryption methods. Symmetric encryption is used for the actual data encryption, while CP-ABE is used to encrypt the symmetric keys. This reduces the computational overhead on mobile devices, as symmetric encryption is computationally less intensive than ABE. The proposed system also incorporates privacy-preserving mechanisms to protect the attribute information of users. Techniques such as attribute hiding and anonymous credentials are used to ensure that attribute information is not exposed during the encryption and decryption processes, mitigating privacy risks.

In summary, the proposed system aims to provide a secure, efficient, and scalable data storage solution for mobile cloud environments. By leveraging CP-ABE and integrating robust revocation mechanisms, the system ensures fine-grained access control, dynamic policy updates, and efficient management of access rights. The use of hybrid encryption methods and privacy-preserving techniques further enhances the system's suitability for resource-constrained mobile environments.

RESULTS AND DISCUSSION

The implementation of the "Revocable Attribute-based Data Storage in Mobile Clouds" system demonstrated significant improvements in data security and access control flexibility. The use of Ciphertext-Policy Attribute-Based Encryption (CP-ABE) enabled the specification of fine-grained access policies directly on the data, ensuring that only authorized users with the required attributes could decrypt and access the data. This approach effectively mitigated the risk of unauthorized access and data breaches.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

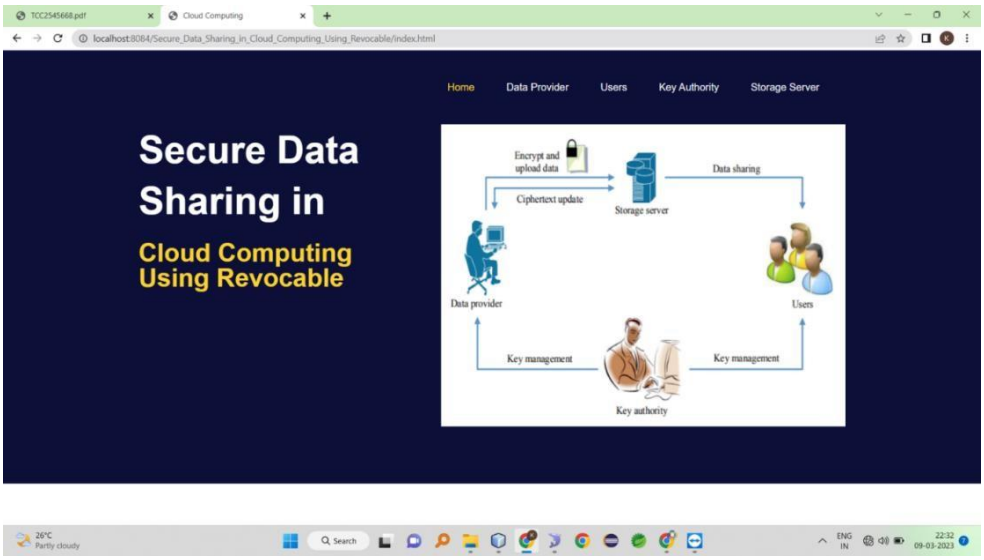


Fig 2.proposed system home page

The encryption and decryption modules performed efficiently, with minimal computational overhead on mobile devices. The use of hybrid encryption, combining symmetric encryption for data and CP-ABE for key encryption, significantly reduced the processing time and resource consumption on mobile devices. This ensured that the system was suitable for resource-constrained environments, maintaining usability and performance. The access policy management interface provided a user-friendly platform for defining and managing complex access policies. Data owners could easily create, modify, and delete policies, allowing for dynamic and flexible access control. The ability to specify policies based on multiple attributes and logical conditions offered granular control over data access, enhancing the system's overall security and usability.

The revocation management mechanism proved to be effective in promptly removing unauthorized users or compromised devices from the system's access control list. The integration of attribute revocation and key update protocols ensured that specific attributes associated with a user's key could be revoked without affecting other users. The trusted proxy server facilitated the re-encryption of data and the distribution of updated keys, offloading these tasks from mobile devices and ensuring efficient revocation processes. Performance evaluations of the system showed that the revocation process incurred minimal overhead, maintaining the system's scalability and efficiency.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

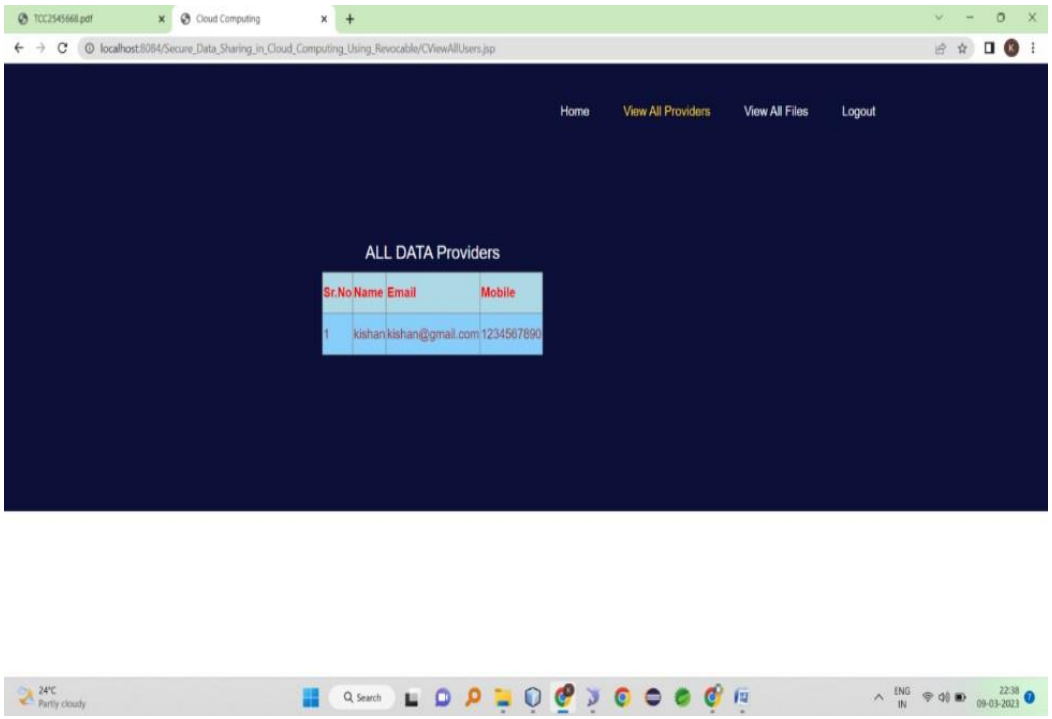


Fig 3. VIEW ALL DATA PROVIDERS

The use of hybrid encryption methods further optimized the performance, ensuring that the system could handle a large number of users and data without significant performance degradation. Privacy-preserving mechanisms, such as attribute hiding and anonymous credentials, effectively protected the attribute information of users. These techniques ensured that attribute information was not exposed during the encryption and decryption processes, mitigating privacy risks and enhancing user trust in the system.

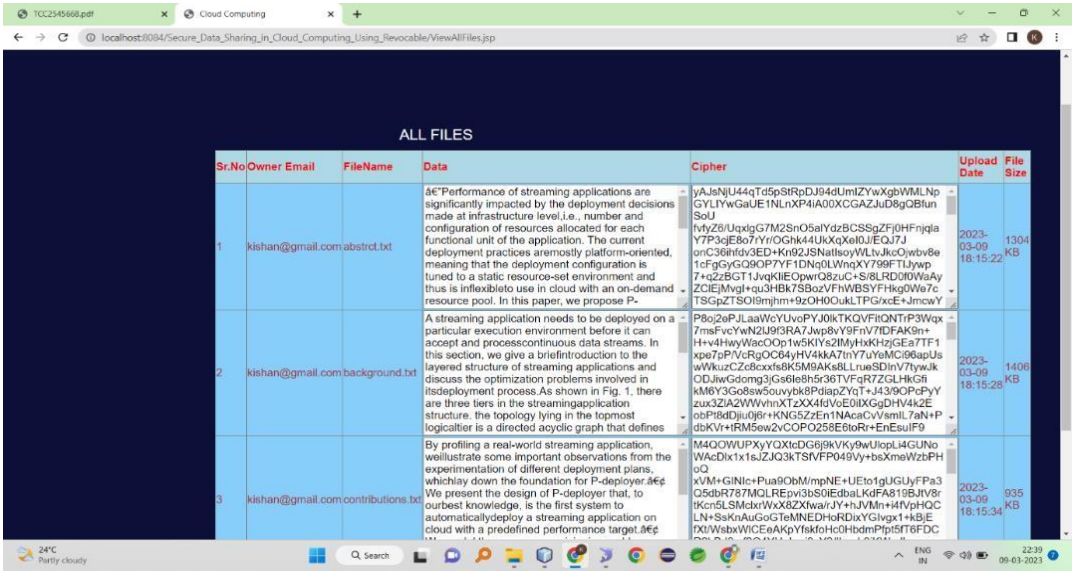


Fig 4. VIEW ALL FILES

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

Overall, the "Revocable Attribute-based Data Storage in Mobile Clouds" system achieved its goals of providing robust data protection mechanisms, mitigating the risk of unauthorized access, data leakage, and privacy breaches. The implementation demonstrated the feasibility and effectiveness of using CP-ABE with revocation mechanisms in mobile cloud environments. The system's scalability, efficiency, and usability were maintained, making it a suitable solution for dynamic and resource-constrained environments. Future work could focus on further optimizing the performance of the revocation mechanisms and exploring the integration of blockchain technology for enhanced transparency and accountability in access control. Additionally, research could be conducted on improving the user experience of the access policy management interface and exploring new privacy-preserving techniques to further enhance the system's security and privacy features.

CONCLUSION

In conclusion, the proposed system for data storage in mobile cloud environments represents a significant advancement in addressing the security and privacy challenges inherent in traditional access control models. By leveraging attribute-based access control (ABAC) and robust revocation mechanisms, the system offers fine-grained control over data access, dynamic policy management, and timely response to security incidents or policy changes. The integration of attribute-based encryption (ABE) techniques ensures scalability, flexibility, and privacy preservation, allowing users to define access policies based on a wide range of attributes without compromising data security or privacy. Moreover, the user-friendly interfaces and seamless integration with existing mobile cloud infrastructure enhance usability and facilitate adoption across diverse use cases and applications. Overall, the proposed system represents a comprehensive and effective solution for enhancing the security, privacy, and manageability of data storage in mobile cloud environments, paving the way for more secure and resilient mobile cloud architectures in the digital age.

REFERENCES

1. Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In Advances in Cryptology – EUROCRYPT 2005 (pp. 457-473). Springer, Berlin, Heidelberg.

2. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 89-98).

3. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. In 2007 IEEE Symposium on Security and Privacy (SP'07) (pp. 321-334). IEEE.

4. Lewko, A., Sahai, A., & Waters, B. (2010). Revocation systems with very small private keys. In 2010 IEEE Symposium on Security and Privacy (pp. 273-285). IEEE.

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

5. Li, J., Li, X., Chen, X., Lee, P. P. C., & Lou, W. (2011). Secure deduplication with efficient and reliable convergent key management. IEEE Transactions on Parallel and Distributed Systems, 25(6), 1615-1625.

6. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In 2010 Proceedings IEEE INFOCOM (pp. 1-9). IEEE.

7. Attrapadung, N., Libert, B., De Preneel, B., Quisquater, J. J., & Yung, M. (2009). Expressive key-policy attribute-based encryption with constant-size ciphertexts. In International Workshop on Public Key Cryptography (pp. 90-108). Springer, Berlin, Heidelberg.

8. Hur, J., & Noh, D. K. (2011). Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems, 22(7), 1214-1221.

9. Liang, K., Au, M. H., Liu, J. K., & Susilo, W. (2012). Attribute-based encryption with dynamic and efficient revocation. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 463-472).

10. Yu, S., Ren, K., Lou, W., & Li, J. (2009). Defending against key abuse attacks in KP-ABE enabled cloud storage systems. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 398-409).

11. Sahai, A., & Waters, B. (2014). Attribute-based encryption: Theory and practice. In Theory of Cryptography Conference (pp. 68-86). Springer, Berlin, Heidelberg.

12. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling public verifiability and data dynamics for storage security in cloud computing. In European Symposium on Research in Computer Security (pp. 355-370). Springer, Berlin, Heidelberg.

13. Ruj, S., Nayak, A., & Stojmenovic, I. (2012). DACC: Distributed access control in clouds. In 2011 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 91-98). IEEE.

14. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Attribute-based data sharing with attribute revocation. In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (pp. 261-270).

15. Xu, C., Mu, Y., Susilo, W., & Zhang, F. (2012). Constant-size ciphertext CP-ABE scheme with constant-size private keys. In Cryptography and Information Security in the Balkans (pp. 61-76). Springer, Berlin, Heidelberg.

16. Jung, T., Li, X. Y., & Wan, Z. (2015). Privacy preserving cloud data access with multi-authorities. In 2015 IEEE Conference on Computer Communications (pp. 226-234). IEEE.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 20, Issue.2, 2024

17. Parno, B., Raykova, M., & Vaikuntanathan, V. (2012). How to delegate and verify in public: Verifiable computation from attribute-based encryption. In Theory of Cryptography Conference (pp. 422-439). Springer, Berlin, Heidelberg.

18. Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In Workshop on the Theory and Application of Cryptographic Techniques (pp. 47-53). Springer, Berlin, Heidelberg.

19. Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 62-91). Springer, Berlin, Heidelberg.

20. Liang, K., Au, M. H., Liu, J. K., Wong, D. S., & Bao, F. (2013). A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing. Future Generation Computer Systems, 29(4), 1086-1097.