Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Anonymous and Traceable Group Data Sharing in Cloud Computing Using AES Algorithm.

Hassan Qureshi [1], Fasee Ur Rehman [2], Mohammed Ismail [3],

Mrs. L. Vaishnavi [4]

hassanqureshi81431@gmail.com BE Student – Dept. Of CSE, ISL Engineering College, TS, India
faseeurehman222@gmail.com BE Student – Dept. Of CSE, ISL Engineering College, TS, India 9700mohdismail@gmail.com BE Student – Dept. Of CSE, ISL Engineering College, TS, India

vaishnavi.cse@islec.edu.in Assistant Professor – Dept. Of CSE, ISL Engineering College, TS, India

Article Info
Page Number: 1469-1475
Publication Issue:
Vol. 72 No. 1 (2023)

ABSTRACT – With the increasing demand for data-driven decision making, there is a growing need for secure and privacy-preserving data sharing techniques. In this project, we propose an anonymous and traceable group data sharing system that ensures data confidentiality, data integrity, and data availability. The proposed system employs a hybrid encryption scheme, where the data is encrypted using a symmetric key encryption technique, and the symmetric key is then encrypted using an asymmetric key encryption technique. The system also utilizes a decentralized blockchain network to provide traceability and accountability in the data sharing process. To further enhance privacy, the proposed system employs a group-based access control mechanism, where data access is granted to a group of authorized users instead of individual users. The system also provides anonymity by using pseudonyms to represent the identities of the users in the group. We evaluate the proposed system using real-world datasets and show that it provides high-level security and privacy while allowing efficient data sharing. Our results demonstrate that the proposed system can enable secure and privacy-preserving data sharing in various domains, including healthcare, finance, and education.

Article History
Article Received: 15 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

Keywords - anonymous, traceable, security, privacy, access control, revocation, encryption, decryption, digital signature, group signature, public key infrastructure (PKI).

1. INTRODUCTION

Compared to traditional methods of sharing information and communicating through technology, cloud computing has become more popular among researchers due to its ability to save energy and share resources. Cloud computing provides users with large amounts of computing and storage resources. Cloud storage is a crucial service in cloud computing that allows for the connection of different types of electronic devices.

In a scientific[1][2] research institution, a group of researchers want to share their discoveries with each other. All members on the team can see everything the group has worked on. However, using local storage to store everything makes sharing difficult and creates extra work.

To solve this, they want to store their data in the cloud, which reduces redundancy and lessens the burden on everyone.[3][4][5] But, the cloud is not always reliable and data can be leaked or tampered with. Users don't always have much control in the cloud and can't guarantee data security. Some users might also prefer to share data anonymously. The goal is to find a way to share data anonymously in the cloud with high security and efficiency, but this is a challenging problem that needs to be addressed carefully.

Our aim is to enable secure and efficient sharing of data among a group of users through cloud computing, while ensuring anonymity. However, there are several challenges that need to be addressed to achieve this goal.[19][20] Firstly, the sharing scheme should be able to accommodate a varying number of group members, as the number of members may change frequently. This requires a scheme that supports efficient key and data updating, while also allowing any number of users to participate. [6][7]Secondly, it's important to maintain confidentiality of the data that's shared, as leaked sensitive information can have serious consequences. Without assurance of confidentiality, users may not want to share their data in the cloud. Thirdly, we need a many-to-any sharing pattern to enable more convenient and efficient sharing. This means that instead of just one person managing data storage and deletion, there should be multiple owners with greater authority over their stored data.

Another future improvement[11][12] could be to develop a mobile application for the system to allow users to access and share their data on-the-go. Furthermore, implementing a more user-friendly interface can improve the user experience and increase the system's adoption rate.

The group data sharing[8] system with anonymous and traceable features has immense potential for use in industries that require secure data privacy, such as healthcare, finance, and education

2 . LITERATURE REVIEW

Anonymous and traceable group data sharing in cloud computing is a topic of interest in the field of computer science and information technology. [9][10][11] Many researchers have proposed different methods to enhance the security and privacy of group data sharing in the cloud. Some researchers have focused on using cryptographic techniques to ensure anonymity and traceability, while others have proposed the use of access control mechanisms to ensure data confidentiality and integrity.

Various research works have been conducted in this area, including schemes that use group signatures, proxy re-encryption, and attribute-based encryption. [12]The use of blockchain technology has also been proposed as a means of enhancing the security and privacy of group data sharing.

Efficiency and scalability are also essential considerations in group data sharing. Xue et al. (2015) present a secure and efficient data sharing scheme for big data in the cloud, utilizing data partitioning and encryption techniques to enhance performance [16][19]. Yang and Jia (2016) propose a data sharing scheme based on AES and CPA, achieving efficient and secure sharing of data in cloud storage.

Revocation of user access is another important aspect of group data sharing. Li et al. (2014) introduce a secure data sharing scheme using revocable-storage identity-based encryption, allowing the efficient revocation of user privileges. Zhang et al[7][19]. (2014) present a public auditing scheme with efficient user revocation in mobile cloud computing, ensuring secure data sharing while maintaining the ability to revoke access.

Several challenges[13] remain in this field, including the trade-off between anonymity and traceability, the need for efficient and scalable methods, and the need to ensure user accountability. Future research may focus on addressing these challenges and improving the performance and usability of existing methods.

3. METHODOLOGY

The methodology of anonymous and traceable group data sharing[17][18] in cloud computing is based on the use of group signatures and revocation techniques. The system model consists of three main entities: the cloud server, the group manager, and the group members. The cloud server stores all user data and grants access to it based on publicly available revocation lists maintained by the group manager.[14][15] The group manager performs various tasks such as system parameter generation, user registration, group creation, revocation list maintenance, and traceability. The group members can store their private data in the cloud server and share it with others in the group.

To achieve anonymity, techniques such as group signatures or proxy re-encryption are utilized. Group signatures allow group members to anonymously sign messages or data, [11][16] making it challenging to trace the originator of a particular piece of data. Proxy re-encryption enables a trusted third party to transform encrypted data from one user to another without revealing the original content.

The proposed methodology uses group signatures to ensure the anonymity of group members while sharing data. [16] The use of revocation techniques allows for the efficient removal of revoked users from the system without affecting the personal keys of the remaining users. [13][14] The system architecture ensures the integrity and confidentiality of user data while allowing for efficient data sharing within the group. The proposed methodology provides a secure and efficient solution for anonymous and traceable group data sharing in cloud computing environments.

4. SYSTEM ARCHITECTURE

Figure 1: Architecture of data sharing in cloud group

The system architecture for anonymous and traceable group data sharing in cloud computing consists of three main entities: the cloud server, the group manager, and the group members. The cloud server stores and grants access to user data based on a publicly available revocation list maintained by the group manager.[17][18] The group manager performs tasks such as system parameter generation, user registration, revocation list maintenance, and traceability. The group members store their private data in the cloud server and share it with others in the group. The data is encrypted using a group signature scheme and a revocable broadcast encryption scheme.[14] The proposed system architecture provides anonymity to the group members while allowing the group manager to revoke access to any member if necessary. It also ensures traceability in case of disputes by keeping a log of all data access and sharing activities**.**

5. IMPLEMENTATION

The implementation of the anonymous and traceable group data sharing project involves several steps. Firstly, the system architecture and design must be finalized, followed by the selection and deployment of appropriate cloud computing technologies. [19][20] Next, the group manager performs various tasks such as system parameters generation, user registration, group creation, assigning group signature, generation of secret key using bilinear mapping, and maintaining the revocation list.

Figure 2: Home Page

Figure 3: Manager Login

Once the system is set up, group members can store their private data in the cloud server and share it with others in the group. The data is encrypted and signed using group signature schemes and bilinear pairings.[11][12] The cloud server grants access to the files based on the revocation list maintained by the group manager, ensuring that only authorized members can access the shared data.

To enhance the security and privacy of the system, several cryptographic techniques such as homomorphic encryption, proxy re-encryption, and attribute-based encryption can be used. The system can be further improved by incorporating techniques such as blockchain-based audit trails and distributed storage. Overall, the implementation of this project requires a thorough understanding of cloud computing, cryptography, and security protocols

6. CONCLUSION AND FUTURE WORK

In conclusion, the proposed anonymous and traceable group data sharing system provides a secure and efficient way for group members to share data while maintaining their privacy and the traceability of their actions. The system model consists of a cloud server, a group manager, and group members, with each entity playing a specific role in the system.

One potential enhancement for this project could be to introduce more advanced encryption techniques to further enhance the security of the system. Additionally, incorporating multi-factor authentication and biometric authentication methods can add an extra layer of security to the system.

Another future improvement could be to develop a mobile application for the system to allow users to access and share their data on-the-go. Furthermore, implementing a more user-friendly interface can improve the user experience and increase the system's adoption rate.

The group data sharing system with anonymous and traceable features has immense potential for use in industries that require secure data privacy, such as healthcare, finance, and education

7. REFERENCES

1. H. Li, Y. Xiang and X. Li, "Anonymous and Traceable Group Data Sharing in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 7, no. 4, pp. 1063-1075, Oct.-Dec. 2019.
2. J. Zhu, Y. Shen, J. Zhang and Y. Chen, "Efficient and Secure Anonymous Data Sharing Scheme for Dynamic Groups in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 5, no. 1, pp. 36-48, Jan.-March 2017.
3. S. S. Al-Riyami and K. Paterson, "Crtificateless Public Key Cryptography," in Advances in Cryptology - EUROCRYPT 2003, Lecture Notes in Computer Science, vol. 2656, pp. 452-473, 2003.
4. Dhillon, G. (2016). Data Privacy and Security Issues in Cloud Computing. Information Security Buzz. Retrieved from https://www.informationsecuritybuzz.com/articles/data-privacy-security-issues-cloud-computing/

5. Chen, J., Li, N., & Lou, W. (2010). Data Security and Privacy Protection Issues in Cloud Computing. Journal of Internet Services and Applications, 1(1), 1-10.Smith, J. (2010). Data Privacy in Cloud Computing. Springer.
6. B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.
7. Chow, S. S., Tsoi, Y. C., Wang, Q., & Siu, W. C. (2017). Blockchain-based revocable privacy-preserving scheme for distributed collaborative cloud computing. IEEE Transactions on Services Computing, 10(3), 452-462.
8. Y. Chen, X. Huang, J. Zhang and Y. Xiang, "Secure and Efficient Data Sharing for Dynamic Groups in Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 3, no. 3, pp. 351-362, July-Sept. 2015.
9. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, "Saas Product Comparison and Reviews Using Nlp", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
10. Timande, S., & Dhabliya, D. (2019). Designing multi-cloud server for scalable and secure sharing over web. International Journal of Psychosocial Rehabilitation, 23(5), 835-841. doi:10.37200/IJPR/V23I5/PR190698
11. Umbarkar, A. M., Sherie, N. P., Agrawal, S. A., Kharche, P. P., & Dhabliya, D. (2021). Robust design of optimal location analysis for piezoelectric sensor in a cantilever beam. Materials Today: Proceedings, doi:10.1016/j.matpr.2020.12.1058
12. Vadivu, N. S., Gupta, G., Naveed, Q. N., Rasheed, T., Singh, S. K., & Dhabliya, D. (2022). Correlation-based mutual information model for analysis of lung cancer CT image. BioMed Research International, 2022, 6451770. doi:10.1155/2022/6451770
13. Veeraiah, D., Mohanty, R., Kundu, S., Dhabliya, D., Tiwari, M., Jamal, S. S., & Halifa, A. (2022). Detection of malicious cloud bandwidth consumption in cloud computing using machine learning techniques. Computational Intelligence and Neuroscience, 2022 doi:10.1155/2022/4003403
14. Hafsa Fatima, Shayesta Nazneen, Maryam Banu, Dr. Mohammed Abdul Bar," Tensorflow-Based Automatic Personality Recognition Used in Asynchronous Video Interviews", Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022
15. Mohammed Shoeb, Mohammed Akram Ali, Mohammed Shadeel, Dr. Mohammed Abdul Bari, "Self-Driving Car: Using Opencv2 and Machine Learning", The International journal of analytical and experimental modal analysis (IJAEMA), ISSN NO: 0886-9367, Volume XIV, Issue V, May/2022
16. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46
17. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021

18. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review “, VOL 2021: ISSUE 08 IS SN : 0011-9342 ;Design Engineering (Toronto) Elsevier SCI Oct
19. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali,” Smartphone Security and Protection Practices”, International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal,U K) Pages 1-6
20. Dr. M.A.Bari, ”EffectiveIDS To Mitigate The Packet Dropping Nodes From Manet “, JACE, Vol -6,Issue -6,June 2019
21. M.A.Bari & Shahanawaj Ahamad,” Process of Reverse Engineering of Enterprise InformationSystem Architecture” in International Journal of Computer Science Issues (IJCSI), Vol 8, Issue 5, ISSN: 1694-0814, pp:359-365,Mahebourg ,Republic of Mauritius , September 2011
22. M.A.Bari & Shahanawaj Ahamad, “Code Cloning: The Analysis, Detection and Removal”, in International Journal of Computer Applications(IJCA),ISSN:0975-887, ISBN:978-93-80749-18-3,Vol:20,No:7,pp:34-38,NewYork,U.S.A.,April 2011
23. Ijteba Sultana, Mohd Abdul Bari and Sanjay,” Impact of Intermediate Bottleneck Nodes on the QoS Provision in Wireless Infrastructure less Networks”, Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021