2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 979-8-3503-6016-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICACITE60783.2024.10616449

An Innovative Way of Trackable GDS in the Field of CC

Megha Pandey,
Assistant Professor, School of Business and Management, CHRIST (Deemed to be University), Bangalore Yeshwanthpur Campus. Email: megha.pandey@christuniversity.in

Subramani K,
Assistant professor, School of Business and Management, CHRIST (Deemed to be University), Bangalore, Yeshwanthpur campus. Email: subramani.k@christuniversity.in.

Madeswaran A,
Associate professor, School of Business and Management, CHRIST (Deemed to be University), Bangalore Yeshwanthpur campus. Email: Madeswaran.a@christuniversity.in

Hassan M. Al-Jawahry,
The Islamic university, Najaf, Iraq. hassanaljawahry@gmail.com Mallesh Sudhamalla, Assistant Professor, Department of ECE, CMR Technical Campus, Hyderabad, Telangana, India, malleshnarayan@gmail.com

Mallesh Sudhamalla,
Assistant Professor, Department of ECE, CMR Technical Campus, Hyderabad, Telangana, India, malleshnarayan@gmail.com

Neeti Misra,
Department of Management, Uttaranchal Institute of Management, Uttaranchal University, Dehradun 248007, India. neeti.cm@gmail.com

K.Krishna Kumar
Department Of Computer Science and Engineering, SSE, Saveetha Institute of Medical and Technical Science - SIMATS Saveetha University, Chennai , India
krishnakumarkathiresan.sse@saveetha.com

Abstract: It is important to provide security and efficient data exchange in cloud infrastructure and achieve traceability and anonymity of data. mean For high levels of safety and performance in one Anonymously, this article addresses the topic It allows data to be exchanged and stored between members of the same group in the cloud. Proposed arrangement creates unique and traceable group data sharing policies using group signatures and special agreements Strategies to accomplish these goals. this Facilitates anonymous communication between systems Public clouds have many users and. Real people following up when needed. Also, the system implements the main agreement programs to make it easier for team members to. Obtain a shared session key for secure data exchange and storage facilities. Basic generation processes a Symmetric Balanced Incomplete Block Theory (SBIBD), significantly reducing the workload of team members a shared session key must be introduced. In cloud computing contexts, the suggested system guarantees efficiency and security for group data sharing, as shown by theoretical analysis and experimental validation.

Index Terms- Cloud computing, Group data sharing, Data traceability, Anonymity, Group signature

I. INTRODUCTION

Cloud computing has emerged as a pivotal technology due to its resource-sharing capabilities and energy efficiency, attracting considerable attention from academia. With its vast processing and storage capacity, cloud computing serves as a vitallink between various technological elements. Despite its widespread use, group data sharing within cloud environments—where multiple users

collaborate to exchange information—has not received adequate attention, despite its practical implications in various fields such as academic research collaborations, Wireless networks in body regions and electronic health networks.[1-3]

One-to-many and many-to-many are the two principal cloud storage data sharing patterns. Whereas in the latter case, a client allows several customers access to their data. A cluster's customers share access to their data among themselves. Similar to scientific studies Members of organisations frequently have to present their results and. improved outcomes, less duplicated data, and a reduction in the work involved in keeping local archives through the use of cloud computing resources. [4]

However, because of the unpredictability and low cloud user usage, problems with privacy and security of data occur. Our goal is to facilitate the anonymization of group data Make the changes in the cloud to be sure efficiency and safety [5].

We suggest a different strategy to address these issues the concept of sharing data among a group in a cloud computing setting where anonymity and explorability are given priority. We support dynamic adjustments and an adjustable user count with our donations. Using encryption, data secrecy is ensured. To achieve traceability under anonymity by the group they provide signatures and fault-tolerant properties and loyalty services. Effectively addressing these obstacles will benefit us.

The suggested system makes clustering secure and efficient. Cloud data sharing, improves data collaboration, and cooperation in a variety of service applications. Additionally, our methodology is flexible. A route for upcoming creation and application Simple compromise strategies, particularly those that employ the SBIBD (symmetrical equilibrium imperfections block design) method.[6]

II. LITERATURE REVIEW

Several approaches have been established in the literature to manage access and secure data storage in cloud computing systems. To manage remote file systems and create secure data storage and semi-trusted identities, the proxy suggested a way to restore encryption.[7]Even while this technique, which is based on bilinear maps, provides better security assurances, it is still susceptible to rogue users and collusion attacks.[8]

An efficient cloud computing access control technique to lessen these risks.. Their method provides simultaneous scalability and relies on the key control attribute-driven

encryption (KA-ABE) technique., data confidentiality, and fine-grained access control. Every data file is first encrypted using the KA-ABE, which encrypts it with a randomly selected key selected by the user.[9] Authorised users receive access structures and secret keys that are kept up to date by the group manager. Decryption is only possible if the data attribute complies with the access structure. But this approach is not appropriate for many-to-many patterns; it is designed for one-to-many communication networks.[10]

Whileseveral studies emphasise the importance of protecting user privacy The narrow scope of these techniques (e.g., the verifiable secure communication method developed for vehicle-to-grid networks in smart grids) may render them inappropriate for group data sharing in cloud settings.

III. PROPOSED FRAMEWORK

Here, we provide a thorough description of our methodology, which makes use of the SBIBD structure to efficiently share group data while requiring the least amount of processing and communication overhead. SBIBD creation, user registration, and parameter initialization are the three primary phases that make up the startup phase. First, by selecting a security parameter \(l \), a bilinear mapping grouping structure \(\mathbb{G}, G_1, G_2, \hat{e} \) is formed. This initialises the BDH parameter generator. To set generators, hash functions, encryption algorithms, and other system properties, a variety of elements and values are selected at random and computed. Second, every group member registers by giving the group administrator their personal data \(I_{Di} \). The group manager assigns a secret key to each member and maintains user records. Thirdly, by serving as the foundation enabling the method of communication for key generation, the SBIBD structure makes it easier to update keys efficiently depending on the size of the group.[11]

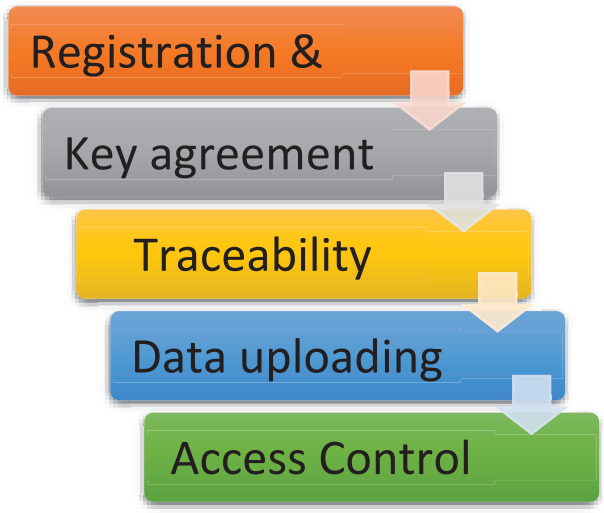

Fig. 1. Framework

Two rounds of key creation are required to produce the group's shared conference key, and the SBIBD structure is used to help in key derivation and efficient communication. Fault detection systems are used to reduce the danger of malevolent members by ensuring that each participant creates a distinct sub-key to avoid interfering with conferences. Verifying the authenticity of messages and spotting differences in key generation are two aspects of fault detection.[12]

Group members encrypt data files using a shared conference key when creating new files and updating keys. After that, they forward the encrypted data to the group's administrator for further processing and verification. Before uploading the data to the cloud, the group manager re-encrypts it using public-key encryption to increase data security and authenticity. To further control member revocation, the group manager employs a revocation list (RL), which keeps banned members from accessing cloud-based data. To maintain data integrity and security in dynamic group settings, Key updating means making changes to the users' shared conferencing key and the private key of the group manager.

Members request permission to view data kept in the cloud from the group management., and the management responds by granting access and sending the required authorization data to the cloud. This process ensures traceability and file access. The group manager's re-encryption key and the authorised members' secret keys allow the latter to decrypt data. Additionally, in the event of a disagreement, the group manager can use master keys to verify signatures and carry out identity lookups to determine the real identities of data holders.[13]

IV. RESULT AND DISCUSSION

We examine the security components of our system in more detail in this section, paying particular attention to data confidentiality, fault tolerance, and anonymity. accessibility and traceability. Our strategy is based on binary Diffie-Hellman (BDH) and discrete logarithm problems (ECDLP) using elliptic curves. The concept of protecting shared data. The dimensions of the state are \(n\) operators, inclusive Potential attackers and volunteers, all as modeled Probabilistic polynomial-time Turing machines, us Deal with the threat posed by the passive enemy, . It is often referred to as the ‘cloud’ of the cloud The goal is to listen to the communication methods for obtaining shared session keys and. Collect information about transferred data. we The method depends on the system parameters {G, P, h2(I). Di)|0 ≤ i ≤ n−1}, with \(r_i\) convergence keys for each User \(i\), protected by ECDLP and BDH measure. Our approach allows for trivial attacks If \(X \ becomes_{\ text {poly}} Y\), record Unobservable polynomial difference between two sets and the random variables \(X\) and \(Y\), \(y \in Z_q^*\) chosen at random. This situation is frightening showing the difference between \(X\) and \(Y\) for each The polynomial-time discrimination is less obvious. as defined in the protection parameter \(l\). As the size of \(p\). Our comprehension ensures error-tolerance. Members find the procedure simpler if there is a shared assembly key. This concludes the discussion. Lemma 3 and Lemma 2 both support it.

Lemma 2 proves that during fault detection, honest group members cannot be removed by others. During fault identification, two situations occur for an honest member \(m\). To begin with, the group manager is notified by \(m\) if \(K_f \neq \prod_{i=0}^{n-1} A_i\), indicating a problem, is detected. Since \(m\) is truthful, there is a member with malicious intent if \(M_g^i \neqA_i\) or \(M_i \neqM_i^*\) exists in \(i\). Furthermore, in the event that the group manager asks for a defect report from \(m\), \(m\) verifies \(M_f^m = A_m\) and \(M_m = M_m^*\), demonstrating the integrity of \(m\). Thus, the group manager's activities have no effect on an honest member. Lemma 3 states that during fault detection, the group manager eliminates hostile participants who try to interrupt the conference. Three scenarios are considered for a

malevolent member \(m\) seeking to disrupt the meeting. In each case, the group manager takes appropriate action to maintain conference integrity, whether by monitoring failure thresholds, detecting inconsistencies in reports, or identifying discrepancies in key usage.[14]

To evaluate performance, we conducted simulations using the GMP Library and PBC Library in our C programming language implementation. Our analysis includes comparisons of efficiency in access control and key generation computational costs between our approach, TPP, and Mona. Figures 2 depict time-cost analyses of signature creation, verification, and overall access control efficiency, respectively, for our system, TPP, and Mona.

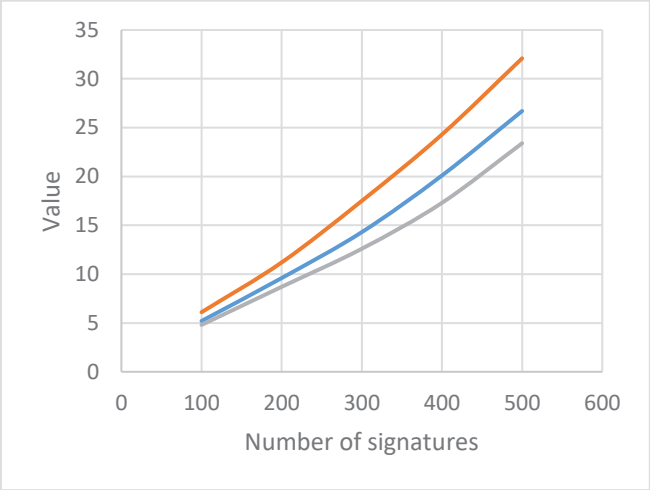

Fig. 2. Efficiency comparison for access control

Our approach demonstrates superior signature creation efficiency and comparable access control efficiency compared to TPP and Mona, making it a favorable choice for practical implementation. Figures 3(a) and 3(b) illustrate the comparison of main generating computational costs between our approach, TPP, and Mona, with and without revoked users. Our method consistently outperforms TPP and Mona in terms of computing efficiency, demonstrating its suitability for data sharing in cloud environments.[15]

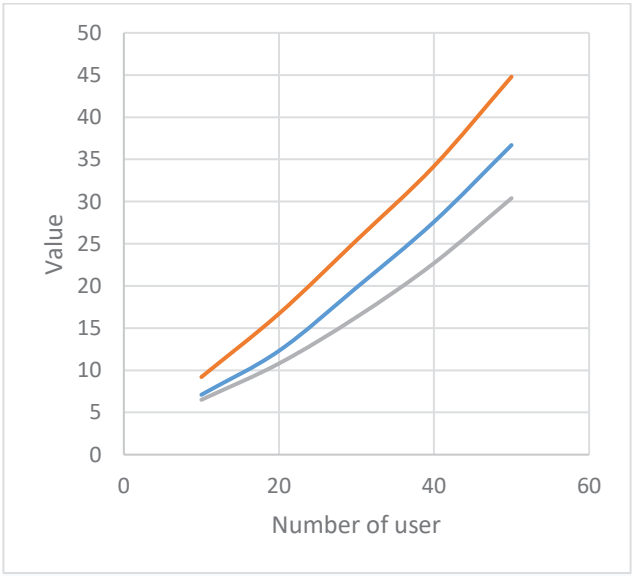

Fig. 3. Comparing the efficiency of key production sans banned customers

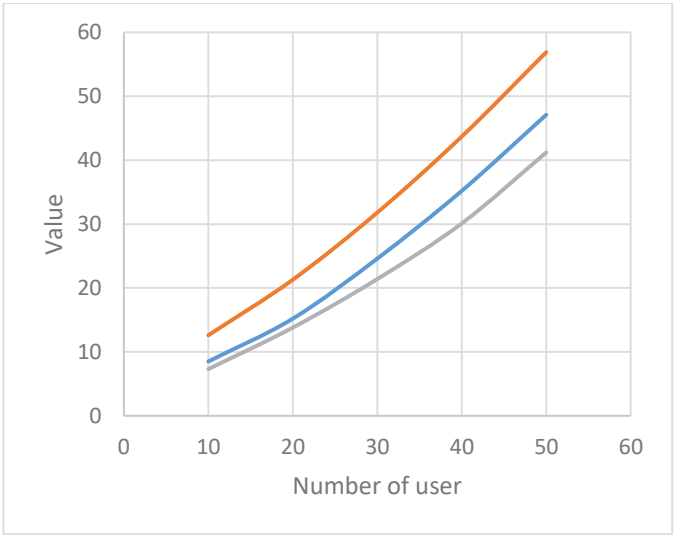

Fig. 4. Efficiency comparision for key generation with 60 revoke users

CONCLUSION AND FUTURE WORK

This project provides the key to robustness and sustainability Compromise methods of cloud storage systems a. Facilitates group data sharing. Our suggestions The method efficiently generates shared sessions key using group signature methods is Incomplete symmetric balanced section system (SBIBD) is. This key has two functions: it protects Confidentiality of data transferred and licensed Secure cloud-based group data. We include a comprehensive mathematical description the Basic ideas of SBIBD and more methods of design. Moreover, our approach provides effective access control and. Authentication services using group signatures The methods of operation. In addition, our system is reassuring Ability to track users anonymously setting. Our methodology minimizes computation and the communication burden of innovation In encrypted data and a shared session key Response to changes by team members through the use of effective special contract programs and prospective access methods.

REFERENCES

[1] A. Santosh Pai Raiturkar, S. Fernandes and A. Pai, "Efficient and Secure Cloud Data Distribution and Sharing Scheme in Groups," 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2018, pp. 157-161, doi: 10.1109/ICOEI.2018.8553711.

[2] T. Makino, Y. Kamidoi and S. Wakabayashi, "A Verifiable Secret Sharing Scheme without Using Multi-Party Computations," 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 2020, pp. 845-850, doi: 10.1109/COMPSAC48688.2020.0-158.

[3] M. A. Islam and S. K. Madria, "Attribute-Based Encryption Scheme for Secure Multi-Group Data Sharing in Cloud," in IEEE Transactions on Services Computing, vol. 15, no. 4, pp. 2158-2172, 1 July-Aug. 2022, doi: 10.1109/TSC.2020.3038836.

[4] A. Fu, S. Yu, Y. Zhang, H. Wang and C. Huang, "NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users," in IEEE Transactions on Big Data, vol. 8, no. 1, pp. 14-24, 1 Feb. 2022, doi: 10.1109/TBDATA.2017.2701347.

[5] S. Patil and R. Patil, "Efficient and Secure Group Data Sharing Model based on Selection scheme in Cloud environment," 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2019, pp. 146-151, doi: 10.1109/ICSSIT46314.2019.8987951.

[6] T. P. Thao, M. S. Rahman, M. Z. A. Bhuiyan, A. Kubota, S. Kiyomoto and K. Omote, "Optimizing Share Size in Efficient and Robust Secret Sharing Scheme for Big Data," in IEEE Transactions on Big Data, vol.

7, no. 4, pp. 703-716, 1 Oct. 2021, doi: 10.1109/TBDATA.2017.2708085.

[7] Q. Li, Q. Zhou, Q. Pan, L. Wang and H. Ding, "A secret sharing scheme based on game theory and BP neural network," 2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys), Nadi, Fiji, 2020, pp. 26-32, doi: 10.1109/DependSys51298.2020.00013.

[8] M. S. Burra and S. Maity, "A Distributed and Decentralized Certificateless Framework for Reliable Shared Data Auditing for FOG-CPS Networks," in IEEE Access, vol. 11, pp. 42595-42618, 2023, doi: 10.1109/ACCESS.2023.3271605.

[9] S. Sivanantham, M. Sakthivel, V. Krishnamoorthy, N. Balakrishna and V. Akshaya, "Reliable Data Storage and Sharing using Block chain Technology and Two Fish Encryption," 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2022, pp. 561-565, doi: 10.1109/ICIRCA54612.2022.9985510.

[10] Lavanya, S., Prasanth, A., Jayachitra, S., Shenbagarajan, A.

[11] Wan, X., Zhang, K., Ramkumar, S., Deny, J., Emayavaramban, G., Siva Ramkumar, M., Hussein, A.F.

[12] Selva, D., Nagaraj, B., Pelusi, D., Arunkumar, R., Nair, A.

[13] Baskar, S., Mohamed Shakeel, P., Kumar, R., Burhanuddin, M.A., Sampath, R.

[14] Velusamy, P., Rajendran, S., Mahendran, R.K., Naseer, S., Shafiq, M., Choi, J.-G.

[15] H. Wang, Y. Zhang, Y. Cheng, Q. Li, J. Zhao and W. Li, "A Data Privacy Protection Scheme Integrating Federal Learning and Secret Sharing," 2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS), Shenyang, China, 2023, pp. 311-315, doi: 10.1109/ICPICS58376.2023.10235406.

[16] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.

[17] R. R. Dornala, S. Ponnapalli, A. R. Lakshmi and K. T. Sai, "An Advanced Cloud Security and Load Balancing in Health Care Systems," 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2023, pp. 1-6, doi: 10.1109/ICSSAS57918.2023.10331892.

[18] T. K. Babu and C. D. Guruprakash, "A Systematic Review of the Third Party Auditing in Cloud Security: Security Analysis, Computation Overhead and Performance Evaluation," 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2019, pp. 86-91, doi: 10.1109/ICCMC.2019.8819848.

[19] P. Sreekumari, "Privacy-Preserving Keyword Search Schemes over Encrypted Cloud Data: An Extensive Analysis," 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS), Omaha, NE, USA, 2018, pp. 114-120, doi: 10.1109/BDS/HPSC/IDS18.2018.00035.

[20] K. P. Singh, V. Rishiwal and P. Kumar, "Classification of Data to Enhance Data Security in Cloud Computing," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 2018, pp. 1-5, doi: 10.1109/IoT-SIU.2018.8519934.

[21] G. Parbu Kanna, Anish Gupta, Yogesh Kumar, Nimisha P Patel “An Enhanced Cloud-Based Healthcare System for Patient Data Privacy and Security Using Hybrid Encryption” in International Conference on Innovative Practices in Technology and Management (ICIPTM), IEEE Sponsored Conference, Amity University, Greater Noida, 23rd – 25th Feb 2022

[22] Ajwad, A.A., Ahmed, A.A., Kamal, M., Jaleel, R.A., & Mahmood, M.B. (2023). Improved Secure IoTs-Based Visual Computing with Image Processing and Artificial Intelligence Techniques for Accurate Predicting of Novel COVID. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14(1), 1-14.