IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 3, June 2025

Impact Factor: 7.67

Attribute -Based Data Sharing Security in Cloud with Data Integrity

Chetana kanifnath Zole[1], Shruti Abaji Urkude [2] , Diksha Pramod Hiradeve [3], Hemant Ghanshyam Khonde [4] ,Neehal Balkrishna Jiwane [5] , Ashish Baban Deharkar

Students, Shri Sai College of Engineering and Technology, Bhadrawati, India[1-4]

Assistant Professor, Shri Sai College Of Engineering and Technology, Bhadrawati, India [5]

Assistant Professor, Somayya Institute of Technology, Chandrapur, India [6]

Abstract: *Cloud computing offers high performance, availability and low cost for data storage and sharing, offers improved utilization of resources. In cloud computing, cloud providers sacrifice an abstraction of unlimited storage space for clients to bulk data. It can assist clients in reducing their capital expense of data managements by moving the local managements system to cloud servers. But security issues arise as our primary limitation since we now outsource storing data, which may be sensitive, to cloud service providers. For maintaining privacy of data, a common technique is to encrypt data files prior to clients uploading the encrypted data to the cloud. Cloud storage solutions can enable clients to minimize their financial and upkeep overhead of data managements. It is difficult to make a secure data sharing plan, particularly for changing groups in the cloud. In order to resolve the issue, here present a secure data sharing method for often updated groups. In this paper, a scheme based on AES encryption is suggested that integrates the cryptographic methods with Group Data Sharing and also an anonymous control method for tackling the privacy in data and also the user identity privacy in existing access control methods. If the member of the group can be revoked means, automatically replace public keys of current group and no longer need encrypt again original data. Any member of group can access data source in cloud and revoked members does not permit accessing the cloud again after revoked. At last integrate this secure distribution scheme into group data sharing systems..*

Keywords: Cloud computing, Data sharing, Security, Privacy Data confidentiality, Data integrity ,Access control

I. INTRODUCTION

The project fully focus on certifying that data shared between multiple users is protected against unauthorized access and tampering, while also allowing users to verify the integrity of the data. The project involves the use of various security mechanisms such as access control, encryption, and digital signatures to provide a secure data sharing environment. Access control mechanisms are used to ensure that only authorized users have access to the data, while encryption is used to protect the data from unauthorized access or interception during transmission. In addition to these mechanisms, the project also uses digital signatures to verify the integrity of the data. Digital signatures are used to ensure that the data has not been tampered with or altered in any way during transmission or storage. This provides an additional layer of security to the data sharing process. Overall, A Secure Data Sharing in Multi User Environment with Integrity Verification project aims to provide a secure and reliable way for multiple users to share data in a way that is protected against unauthorized access and tampering. The project is relevant in various scenarios where multiple users need to access the same data, such as in a corporate or academic setting,and where data security is of utmost importance.Managing and auditing network access is essential to information security. Access can and should be granted on a need-to-know basis. With hundreds or thousands of employees, security is more easily maintained by limiting unnecessary access to sensitive information based on each user’s established role within the organization.

DOI: 10.48175/568

II.RELATED WORK

This paper analyzed though it's a popular IT catchword and ideas are derived from decade old grid computing, distributed computing, utility computing and intensive application computing. It offers a broader range of services such as virtual machines (VMs), servers, storage devices, operating systems (OS), and network resources over the internet to its users on 'pay-for-usage' basis. Active group data sharing were users anonymously share his/her data with other group members over cloud could compromise security hence there is need to design an efficient, secure data sharing in dynamic group. Hence, this review paper presents various problems and challenges in designing an effective dynamic group data sharing. The problems and challenges are secret based on Client based and service provider based were client-based problems includes user authentication, user privacy and security, data confidentiality & integrity and query cost and service provider based problems includes user's identity & traceability, user revocation, energy efficiency and performance. Based on the challenges, researchers have proposed and developed various protocols, management and control mechanisms under data security, access control, query grouping and energy efficiency headings which is briefly summarised in this review to help future researchers in developing efficient, security data sharing schemes in cloud environment.

III. EXISTING SYSTEM

Propose an attribute-based controlled cooperative access control scheme for public cloud storage. Restrict user collaboration in the same group that corresponds to the same project for which the involved people are responsible. Thus, in proposed work, in order to provide both data privacy and collaborative access control, only people who are in charge of the same project are allowed to collaborate. Technically, data owners allow expected collaboration by designating translation nodes in the access structure. In this way, unwanted collusion can be resisted if the attribute sets by which users are collaborating are not corresponded to translation nodes. For each translation node, an additional translation value is generated. Using this translation value and special translation keys embedded in users' secret keys, users within the same group can collaborate to satisfy the access structure and gain the data access permission. For colluding users across groups, their access is not permitted as their secret keys do not correspond to the same group. Users are divided into groups in a way such that the collaboration is restricted and secure. That is to say, only users responsible for the same project are allowed to collaborate in case those malicious users who are not responsible for the project collude. Extensive security analysis is given to show the security properties of our proposed scheme.

In existing scheme, the security assumptions of the four roles can be defined as follows. Cloud servers are always online and are managed by the cloud provider who is usually assumed to be "honest-but-curious". It means that cloud servers will correctly execute the tasks assigned to them for profits, but they would try to obtain as much secret information as possible based on data owners' inputs and outsourced data.

IV. PROPOSED SYSTEM

To enable data sharing in the Cloud, it is essential that only authorized users are able to get access to data stored in the Cloud. When the data owner wants to share their own data to a group, he/she sends the key used for data encryption to each member of the group. Any of the group members can then get the encrypted data from the Cloud and decrypt the data using the key and hence group member does not require the interference of the data owner. The problem in this technique is that it is inefficient. When the data owner gets back the access rights from a member of the group, that member must not be able to access to the corresponding data. Since the unauthorized member of the group still has the data access key. So the data owner has to re-encrypt the data with a new key. When the data is re-encrypted, data owner must give out the new key to the remaining users in the group and this is computation inefficient.

V. METHODOLOGY

The AES cipher is also referred to as the block cipher. Now a successful attack has been noted on AES. Some advantages of AES are smooth to enforce on eight-bit processors and powerful implementation on 32-bit structure processors. AES encryption is performed in multiple rounds. Each round has 4 vital steps in conjunction with sub-byte, shift row, mix column, and upload round key. Sub-byte is the substitution of bytes the use of a lookup-up table. Shift

DOI: 10.48175/568

row is the shifting of rows consistent with byte duration. The Mix column is multiplication over the Galois subject matrix. Finally, inside the upload round key step, the output matrix of the blend column is XORed with the round key. The wide variety of rounds used for encryption is predicated upon at the critical issue size. For a 128-bit key, these 4 steps are applied to 9 rounds, wherein the 10th round does not take into account the aggregate column step. Since all steps are recursive, decryption is the alternative of encryption.

Data Sharing Framework

In this module, create a local Cloud and provide priced abundant storage services. The group managers can add their data within the cloud, wherein the cloud storage can be made at ease. However, the cloud is not fully dependent on by users for the reason that CSP is very probably to be outside of the cloud customers depended on the area. The Proposed secure data sharing framework provides communication between the group manager and the group members.

Group Manager takes charge of followings,

1. System parameters generation
2. User registration
3. User revocation
4. Revealing the original identity of the outsourced group manager.

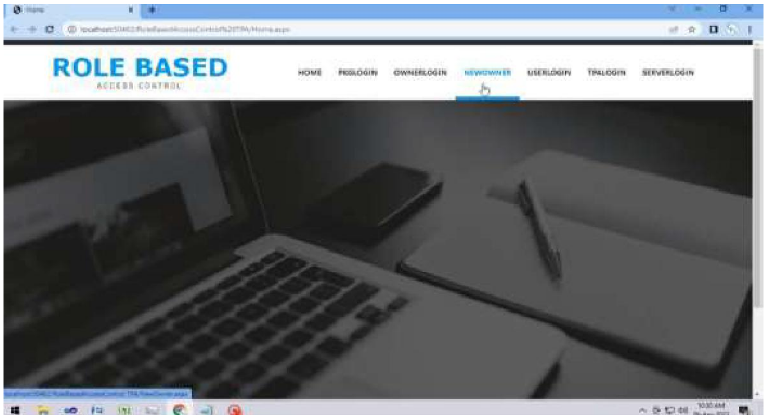
Therefore, the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager should login and upload each and every file in the cloud. The group manager is responsible for every user registration and user revocation too.

Key Generation and Distribution

Key Generation is the process of generating a secret key for group manager and group members. After completion of the registration secret key is generated using a random key generation process and send to the corresponding member through email. During login, a member should enter their secret key that will be verified with the database. If a member does not have valid user id they will not allow accessing an application. The concept of group signatures was performed by PKG (Public Key Generation). Informally, a group signature scheme permits any member of the group to sign messages even as retaining the identity secret from verifiers. Besides, the certain institution manager can reveal the identity of the signature's originator when a dispute happens, which is denoted as traceability. In this paper, a variant of the group signature updation scheme will be used to achieve anonymous access control, as it supports efficient membership revocation.

VI. EXPERIMENTAL RESULT

The Experimental result shows the overall performance of the proposed system. Here Role-based access control for data sharing and auditing schemes are implemented using ASP.NET as front end and SQL as back end Software.



The above figure is interface of a secure group data sharing

VII. CONCLUSION

Data sharing in the Cloud is available in the future as demands for data sharing continue to grow rapidly. Proposed work, presented a review on secure data sharing in cloud computing environment. To reduce the cost data owner outsource the data. Data owner is unable to control over their data, because cloud service provider is a third party provider. The problem with data sharing in the cloud is the privacy and security issues. Various techniques are discussed in this paper to support privacy and secure data sharing such as AES encryption, Group data sharing and User revocation. The study concludes that secure anti-collision data sharing scheme for groups provides more efficiency, supports access control mechanism and data confidentiality to implement privacy and security in group sharing.

REFERENCES

[1]. Kotha, Sita Kumari, Meesala Shobha Rani, Bharat Subedi, Anilkumar Chunduru, Aravind Karrothu, Bipana Neupane, and V. E. Sathishkumar. "A comprehensive review on secure data sharing in cloud environment." Wireless Personal Communications 127, no. 3 (2022): 2161-2188.

[2]. Khashan, Osama Ahmed. "Secure outsourcing and sharing of cloud data using a userside encrypted file system." IEEE Access 8 (2020): 210855-210867.

[3]. Chen, Biwen, Libing Wu, Li, Kim-Kwang Raymond Choo, and Debiao He. "A parallel and forward private searchable public-key encryption for cloud-based data sharing." IEEE Access 8 (2020): 28009

[4]. Sandhya.S. Bachar, Neehal.B. Jiwane, Ashish.B. Deharkar "Sentiment analysis of social media" DOI: 10.17148/IJARCCE.2022.111234 International Journal of Advanced Research in Computer and Communication Vol. 11, Issue 12,□□Impact Factor 7.918□□Engineering ISO 3297:2007 Certified December 2022.

[5]. Atharv Arun Yenurkar , Asst Prof. Neehal B. Jiwane , Asst. Prof. Ashish B. Deharkar. "Effective Validation for Pervasive Computing and Mobile Computing Using MAC Algorithm". International Journal of Research Publication and Reviews, Vol 3, no 12, pp 470-473 December 2022