IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105133

A Survey Based on Secure Audit Mechanism for Data Sharing on Cloud Storage

Ganesh Magar[1], Prajwal Waghmare[2], Pankaj Ghaywat[3]

B.E Students, TSSM'sBhivrabai Sawant College of Engineering and Research Narhe Pune,Savitribai Phule University, Pune,Maharashrta,India[1-3]

Abstract:As data sharing has become one of the most popular services offered by cloud storage, designing public auditing mechanisms for integrity of shared data become more important. Two problems which arise In shared data auditing include preserving users identity and collusion resistant revocation of users. To ensure the security of data sharing within group and outsourced data in group manner are formable challenges. The key protocols have played a very important role in secure and efficient group in cloud computing. To solve this problem, Symmetric balanced incomplete block design (SBIBD) are used for key Security and un-authorized user can't access the Data from different group. SBIBD is used the general formula for generating the common conferences key K for multiple Participants. General formula (v,K+1,1) block design is used to data are stored. As Result of storing datafrom dynamic group and Data are divided Block and System Performances are a better as compared to Exiting Scheme with help of algorithm Blows fish and DES and Encryption used as fully Homomorphism encryption.

Keywords: Cloud storage auditing, cloud storage, outsourcing computing, key update, encryption.

I. INTRODUCTION

In Cloud Computing Data Sharing empowers various members to unreservedly share the diverse gathering information, which broadly enhance the proficient of work in helpful. Instructions to guarantee the security of information sharing inside gathering and redistributed information in gathering way are formable difficulties. The Key conventions have assumed an essential job in secure and effective gathering in distributed computing. To take care of this issue in this paper, Symmetric adjusted inadequate square structure (SBIBD) are utilized for key Security and un-approved client can't get to the Data from various gathering. SBIBD is utilized the general recipe for producing the basic meetings key k for different Participants. General recipe (v, K+1, 1) square structure is utilized to information are put away. As Result of putting away information from dynamic gathering and Data are partitioned Blocks and System Performances are a superior when contrasted with Exiting Scheme with help of best calculations is Blow fish and DES and Encryption utilized as completely Homomorphism encryption.

II. MOTIVATION

The Main Aim in Secure cloud audit is to Share the Data with Sensitive Information hiding and Block level data storing with homomorphism encryption

III.REVIEW OF LITERATURE

1. Secure Attribute–based data sharing for resources-limited users in cloud computing, this system has used potential technique for realizing fine-grained data sharing, attribute-based encryption (ABE) . This paper proposes a new attribute-based data sharing scheme suitable for resources-limited mobile user in cloud computing. The proposed system eliminates a majority of computation task by adding system public parameters besides moving partial encryption computation offline. The proposed system is proven secure against adaptively chosen ciphertext attacks, which widely recognized as a standard security notion

2. Anonymous Data Sharing Scheme in Public Cloud and its Application in E-Health Record, A large amount of data are uploaded and stored in public cloud servers which cannot fully be trusted by users. When the data outsourced in the cloud are sensitive, the challenges of security and privacy of data becomes urgent. This paper proposes a secure data sharing scheme to ensure the privacy of data owner and security of the outsourced cloud data. The proposed scheme provides flexible utility of data while solving the privacy and security challenges for data sharing. The security and efficiency analysis demonstrate that the designed scheme is feasible and efficient. At last, we discuss its application in electronic health record.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105133

3. Public key encryption with keyword search. We consider the issue of looking for on data that is encoded using an open key system. Consider customer Bob who sends email to customer Alice mixed under Alice's open key. An email entryway need to test whether the email contains the catchphrase "sincere" with the objective that it could course the email fittingly. As another portrayal, consider a mail server a key that will empower the server to see all messages containing some explicit catchphrase, in any case get nothing else. We depict open key encryption with watchword demand and give two or three enhancements.

4. Lightweight and efficient data sharing scheme for cloud computing, Nowadays Attribute Based Encryption(ABE) is widely used to probide secure data sharing in the distributed environment such as cloud computing. Unfortunately most of existing Abe schemes are not suitable for resource constraint cloud systems. In this paper, they propose an efficient no-pairing and revocable ABE data sharing scheme based on Elliptic Curve Cryptography (ECC) for cloud storage systems. Moreover, a comprehensive security and performance analysis shows that our scheme is both secure and efficient

5. Secure Keyword Search and Data sharing Mechanism for cloud computing, this system propose a ciphertext-policy attribute based mechanism with keyword search and data sharing(CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute based keyword search but also enables attribute based data shaing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in this scheme can be updated during the sharing phase without interacting with the PKG. In this paper, they describe the notion of CPAB-KSDS as well as its security model. They propose a concrete scheme and prove that it against chosen ciphertext attack and chose keyword attack secure in the random oracle model.

6. Anonymous hierarchical identity-based encryption, In this paper they demonstrate a character based cryptosystem that feature totally obscure cipher texts and different levelled key assignment. They prove security in standard model, in light of delicate Decision Linear multifaceted nature supposition in bilinear get-togethers. The system is powerful and helpful, with little cipher texts of size direct in the significance of the chain of significance. Applications join interest on encoded data, totally private correspondence, etc. The result settle two open issues identifying with obscure character based encryption, arrangement being the first to offer provable mystery in standard model, despite being first to recognize totally strange HIBE at all dimensions in the Chain of importance.

7. **An Data Sharing In Group with High Security Using Symmetric** B**alanced Incomplete Block Design (SBIBD) In Cloud Computing,** This paper centers on empowering information allocation as well as capacity pro a similar gathering in cloud through high security as well as effectiveness in an unknown way. By utilizing the key understanding as well as gathering mark, a novel detectable gathering information sharing plan is proposed to help mysterious various clients in open mists. As a symmetric adjusted fragmented square structure is used pro key age, which considerably lessens the weight on individuals to determine a typical gathering key. Both hypothetical as well as test examinations show so as to the proposed plan is secure as well as proficient pro gathering information partaking in distributed computing

8. **Practical techniques for searches on encrypted data,** It is alluring to store information on information stockpiling servers, for example, mail servers and record servers in encoded shape to diminish security and protection dangers. Yet, this as a rule suggests that one needs to forfeit usefulness for security. For instance, if a customer wishes to recover just archives containing certain words, it was not already known how to let the information stockpiling server play out the inquiry and answers the questions without loss of information classification

IV.PROPOSED WORK

In Our System proposed an identity-based data integrity auditing scheme for secure cloud storage, which supports data sharing with sensitive information hiding. In our Application doctor upload the data into cloud with user and researcher when Doctor Share the data with User that file go to Admin and admin convert into Binary format and after that binary format file again convert into Homomorphic encryption and Stored into Block Level.

In System there are six roles such as the Doctor and Sanitizer (Admin) and Patient (User) and Researcher and TTP (Trust Third party) and PKG (Private Key Generated) First in System Doctor upload the Report According to their choice of User and Researcher if Doctor Select the Patient Upload the Report with patient ID after uploading Sanitizer Convert the Data into Binary format using Specialized Algorithms. After converting into Binary part Cloud Server provider is stored the Data into Homomorphic Encryption and Copy into Block Level. At that Cloud Server provider

IJARCCE

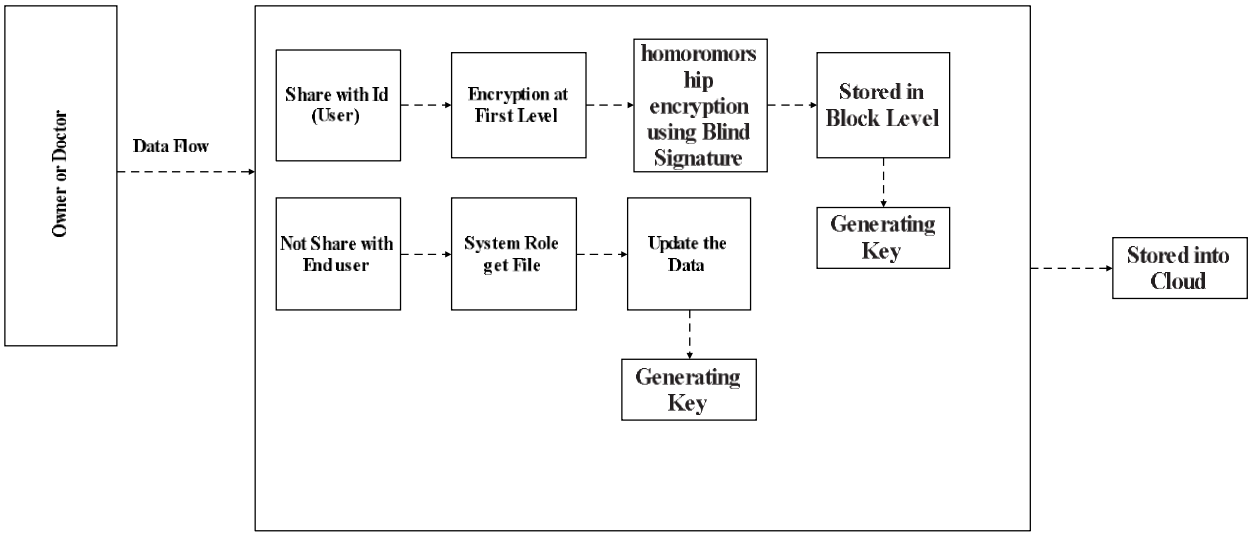
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.105133

V.ARCHITECTURE



VI.ADVANTAGES

- Usability and accessibility.
- Security.
- Cost-efficient.
- Convenient sharing of files.
- Automation.
- Synchronization.
- Convenience.

VII.CONCLUSION

The research work proposes and illustrate data sharig within the cloud environment instead of employing cloud storage devices. Using this secure and efficient auditing technique, data can be safeguard against the auditor. In contrast to the mask technique, the blend of cryptography method proves to be effective tool for securing huge amount of owner's data. Hence any additional organizer is not required for auditing purpose in multi-owner storages. The security proof and the experimental analysis demonstrate that the proposed scheme achieves desirable security and efficiency

VIII.REFERENCES

1. Secure keyword search and data sharing mechanism for cloud computing Chunpeng Ge, Willy Susilo, Zhe Liu, Jinyue Xia, Pawel Szalachowski, Fang Liming IEEE
4. lightweight and efficient data sharing scheme for cloud computin Majid Bayat, Mohammadali Doostari, Saeed Rezaei International Journal of Electronics and Information Engineering 9 (2), 201
5. AN DATA SHARING IN GROUP MEMBER WITH HIGH SECURITY USING SYMMETRIC BALANCED INCOMPLETE BLOCK DESIGN (SBIBD) IN CLOUD
.Kulkarni[1], Bhagyashri N.Ghatke International Research Journal of Engineering and Technology(IRJET)e-ISSN: 2395-0056Volume: 06 Issue: 09 | Sep 2019 Transactions on Dependable and Secure Computing, 2020.
2. Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-Health Record Huaqun Wang IEEE Access 6, 27818-27826, 2018
3. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp.
2402–2415, Oct. 2017.