International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Untraceable Group Data Sharing for Secure Cloud

[1*]T Santosh, [2]P Cefhora, [3]T Chandana
[1]Associate Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India
[2,] Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

Article Info
Volume 9, Issue 5
Page Number : 311-316

Publication Issue :
September-October-2022

Article History
Accepted : 01 Oct 2022
Published: 22 Oct 2022

ABSTRACT

Cloud computing is nothing but delivering applications as services over internet and these services are provided by combination of hardware's and software's of data center's and these services as Saas, Paas,Iaas etc. cloud computing commonly describe as converting capital expenses into operating expenses (CapEx to OpEx. Cloud computing provide ability to store data in cloud and share that valuable data to multiple authorized users. It also provides economical and efficient solution for sharing group resources among multiple cloud users. Sharing data among multiple users' lights on defensive of data and identity privacy of users from untrusted cloud is still challenging problem. Encrypting documents with different keys using public key cryptosystem such as Attribute based encryption (ABE) and Proxy re-encryption has some weaknesses. It can't efficiently handles adding or revoking users or identity attributes. In this paper we proposed a secure, efficient data sharing scheme for dynamic groups in cloud with anonymous authentication of cloud users. By combining group signatures and dynamic broad encryption technique, any cloud user will anonymously share data with other users efficiently. There are some issues regarding storage overhead and encryption computation costs are overcome here.

Keywords: Clouding Computing, Data Sharing, Privacy Preserving, Access Control, Dynamic Groups.

I. INTRODUCTION

Basically cloud means data center's hardware and software's. Cloud computing refers to manipulating, configuring and accessing both hardware and software resources from remote location [1].Using cloud computing one can store, share his/ her data to other trusted parties in cloud. To protect data privacy in the cloud, sensitive data, for example, e-mails, personal health records, photo albums, tax documents, financial transactions, and so on, may have to be encrypted by data owners before they are getting to outsourcing to the commercial public cloud [2].By applying cryptography methods for data encryption, keep sensitive data confidential against untrusted cloud server. Further disclosing data decryption keys to

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

authorized users only, but this solution introduce heavy computation overhead on data owner for key distribution. [3] Allowing data owner to depute untrusted cloud server in fine grained access control without disclosing the underlying data contents. There are some problem related to secure and efficient data sharing for dynamics groups in cloud are as: Now a day's user's identity privacy is major concern. Without guarantee of identity privacy, user may not confident to store data in cloud storage. If we see on other side unconditional users identity privacy leads to snap up to privacy. Due to this issues traceability allow group manager to show the identity of user when any dispute occurs. Secondly any member in group should capable of data storing and sharing services [3] allow only group manager to store, modify data in the cloud but in multi-owner manner, every user in group can store, share and modify his/ her part of data in entire data file shared by the company. Lastly in any system dynamically user registration and revocation should smoothly occur. In [6] many security scheme are proposed. In their approaches, data owners store his/her data in cloud and distribute corresponding decryption keys to authorized users but these schemes had some drawbacks related to user registration and revocation. Secure provenance scheme [7] based on bilinear mapping technique to provide trusted evidence data forensics. [8] Proposed cipher text policy attribute based encryption technique allowing any member in group to share data with other members but revocation problem is not solved in above scheme. Fine grained access control achieving through key policy attribute based encryption [7].In this paper we proposed secure, efficient data sharing scheme which allow user to securely share his/her data to other by untrusted cloud server. Proposed scheme has some advantages includes, it provides dynamic group sharing, user revocation is made easy, computation overhead of encryption does not corresponds to number of revoked users. Any user in group can anonymously share data files to other. But any dispute will occur; data manager can reveal his/her identity by group signature.

II. LITERATURE SURVEY

Defines cloud refers to data center's hardware and software. They describes obstacles and opportunities in cloud computing. It focuses on encrypting sensitive information before it is outsourced to untrusted cloud storage. They also lights on various architecture of cryptographic storage services like a consumer of cryptographic storage architecture, enterprise architecture. It proposed cryptographic cloud storage system that enables secure file sharing on untrusted cloud server and that system named as "Plutus". File get divided into file-groups and encrypting each file group with unique file block key and then data owner can share the file groups with others through lockbox key, this lockbox key generally used for encrypting file-block keys. But it has some drawbacks includes file-block keys need to be updated and distributed again for user revocation [1]. It proposed a security mechanism that improves the security of a network file system without making any changes to the file system or network server. In Sirius, files have two parts: File metadata and file data, stored on untrusted server. The file metadata has the access control information including a series of encrypted key blocks and these key blocks are encrypted under the public key of authorized users. But the size of metadata increased with number of authorized users. Revocation and tracing solved the problem of efficient key revocation by NNL construction. But it didn't support for dynamics groups in clouds besides that computation overhead of encryption increases linearly with the sharing scale[2]. Proxy Re-Encryption allows a proxy to transform a cipher text computed under Alice's public key into one that can be open by Bob's secret key. Using Proxy Re-Encryption scenario data owner encrypts block of content with unique and symmetric keys and further these symmetric content keys are encrypted under a master public key. For providing access control, cloud server uses Proxy Re-Encryption for directly re-encrypt appropriate contents key from master public key to allowing users public key. Due to this method malicious revoked user can read decryption keys of encrypted content blocks. In an ABE system, a user's keys and ciphertexts are labelled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. A secure, scalable and fine-grained data access control scheme is based on the combination of KP-ABE, Proxy Re-Encryption, and Lazy Re-Encryption technique. KP-ABE allows data owner to delegate computation tasks for providing access control to untrusted cloud servers without disclosing actual data contents. Also user secret key updating process delegated to cloud server by group manager. So it is somewhat advantageous regarding computation overhead on server not on client side. But KP-ABE scenario did not provide multiple owner data sharing [3].

Secure provenance scheme based on bilinear mapping, group signatures and cipher text policy based encryption techniques. The system in their scheme is characterized by providing the information confidentiality on sensitive documents stored in cloud, anonymous authentication on user access and provenance tracking on dispute documents. In provenance technique a data object can report who created and who modified its contents. Therefore, once a dispute rises in a document stored in cloud, provenance is important for data forensics to provide digital evidences for post investigation. User revocation is not suitably implemented inShort group signature provides anonymity of data owner. The system in their scheme is based on strong Diffie-Hellman assumptions. For privacy preserving in data sharing, group signatures are needed. From the above analysis it is clear that we want a system that provides efficiency, security, access control, user’s identityprivacy during storing and sharing data by cloud server [4].

It proposed a security for customers to store and shares their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. HoIver, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and re-publish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data. They have applied the efficient revocation scheme to the cipher textpolicy attribute-based encryption based cryptographic cloud storage. The security analysis shows that the scheme is computationally secure [5].

III. PROPOSED SYSTEM

The goal of this project is to develop a secure multi-owner data sharing method. It implies that any group member can securely communicate data with others through an un trusted cloud. The proposed approach can effectively support dynamic groupings. Newly granted users, in particular, can directly decrypt data files uploaded prior to their involvement without having to contact data owners. User revocation is simple to accomplish using a novel revocation list that does not require upgrading the secret keys of surviving users. The size and computation overhead of encryption remain constant and unaffected by the number of users whose access has been revoked .Provide users with safe and privacy-preserving access control, ensuring that any group member can use the cloud resource anonymously .Perform a thorough security analysis and demonstrate the scheme's efficiency in terms of storage and compute overhead.

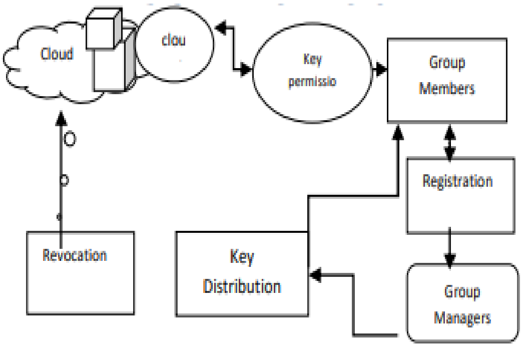

Fig1: System Architecture

If a member want to join the group, they must first register as a member. Only the manager can activate a new member after registration is complete, so a new member cannot login without access. Following the update, a group member can now upload a file, which generates a 16-bit key that is sent to the group member through SMTP protocol via email. The user can only read or write files with that key. Revocation is utilized if a user needs to remove a file, and the data is saved in the cloud.

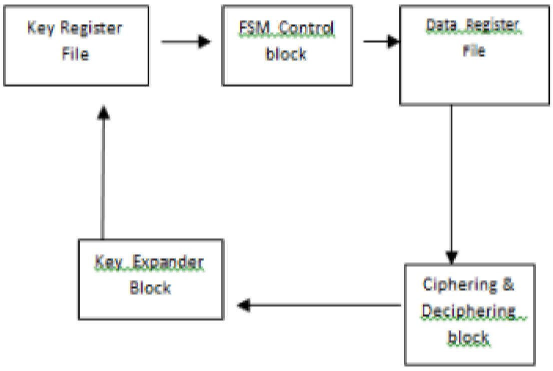

Fig 2: Block Diagram

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

ALGORITHM

AES

The AES Encryption algorithm (also known as the Rijndael algorithm) is a symmetric block cipher algorithm with a block/chunk size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. Once it encrypts these blocks, it joins them together to form the cipher text.

High-level description of the algorithm

1. Key Expansion:

Round keys are derived from the cipher key using Rijndael's key schedule

2. Initial Round

Add Round Key—each byte of the state is combined with the round key using bitwise xor

3. Rounds

Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.

Mix Columns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

Add Round Key

4. Final Round (no Mix Columns)

Sub Bytes

Shift Rows

Add Round

IV. CONCLUSION AND FUTURE WORK

As a response, erasure coding as an alternative to backup has emerged as a method of protecting against drive failure .Raid just does not cut it in the age of high-capacity HDDs. The larger a disk's capacity, the greater the chance of bit error .And when a disk fails, the Raid rebuild process begins, during which there is no protection against a second (or third) mechanism failure. So not only has the risk of failure during normal operation grown with capacity, it is much higher during Raid rebuild, too. Also, rebuild times were once measured in minutes or hours, but disk transfer rates have not kept pace with the rate of disk capacity expansion, so large Raid rebuilds can now take days or even longer. As a response, erasure coding as an alternative to backup has emerged as a method of protecting against drive failure .Raid just does not cut it in the age of high-capacity HDDs. The larger a disk's capacity, the greater the chance of bit error .And when a disk fails, the Raid rebuild process begins, during which there is no protection against a second (or third) mechanism failure. So not only has the risk of failure during normal operation grown with capacity, it is much higher during Raid rebuild, too. Also, rebuild times were once measured in minutes or hours, but disk transfer rates have not kept pace with the rate of disk capacity expansion, so large Raid rebuilds can now take days or even longer.

We would like to express a deep sense of gratitude towards our guide Mrs.R.Yugha, Assistant Professor of information Technology Department for her constant encouragement and valuable suggestions. The work that we can present is possible because of her timely guidance.

V. REFERENCES

[1] Dr .K. Kartheeban , A.Durai Murugan "Privacy Preserving Data Storage Technique in Cloud Computing" 2017 IEEE INTERNATIONAL CONFERENCE ON INTELLIGENT TECHNIQUES IN CONTROL, OPTIMIZATION AND SIGNAL PROCESSING 978-1-5090-4778-9/17/$31.00 ©2017 IEEE

[2] Haifeng Lu, Chuan Heng Foh, Yong gang Wen, and Jianfei Cai, "Delay-Optimized File Retrieval under LTBased Cloud Storage", IEEE transactions on cloud computing, vol. 5, no. 4, october-december 2017

[3] Yong Cui , Zeqi Lai, Xin Wang, and Ningwei Dai," QuickSync: Improving Synchronization Efficiency for Mobile Cloud Storage Services", IEEE transactions on mobile computing, vol. 16, no. 12, december 2017

[4] Hui Tian, Yuxiang Chen, Chin-Chen Chang,Hong Jiang, Yongfeng Huang, Yonghong Chen, and Jin Liu," Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage", IEEE transactions on services computing, vol. 10, no. 5, september/october 2017

[5] Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han," KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage", IEEE transactions on services computing, vol. 10, no. 5, september/october 2017

[6] Guoxin Liu and Haiying Shen, "Minimum-Cost Cloud Storage Service Across Multiple Cloud Providers", IEEE/ACM transactions on networking, vol. 25, no. 4, august 2017

[7] Guoxin Liu, Haiying Shen, and Haoyu Wang, " An Economical and SLO-Guaranteed Cloud Storage Service Across Multiple Cloud Service Providers", IEEE transactions on parallel and distributed systems, vol. 28, no. 9, september 2017

[8] Jianwei Yin, Yan Tang, Shuiguang Deng, Ying Li, Wei Lo, Kexiong Dong, Albert Y. Zomaya, and Calton Pu," ASSER: An Efficient, Reliable, and Cost-Effective Storage Scheme for Object-Based Cloud Storage Systems", IEEE transactions on computers, vol. 66, no. 8, august 2017.

[9] Mazhar Ali, , Saif U. R. Malik, and Samee U. Khan, " Data Security for Cloud Environment with SemiTrusted Third Party"IEEE transactions on cloud computing, vol. 5, no. 4, october-december 2017

[10] Anmin Fu, Shui Yu, Yuqing Zhang, Huaqun Wang, and Chanying Huang," NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users" , © 2017 IEEE Transactions on Big Data.

[11] Nicolae Paladi, Christian Gehrmann, and Antonis Michalas," Providing User Security Guarantees in Public Infrastructure Clouds" IEEE transactions on cloud computing, vol. 5, no. 3, july-september 2017

[12] Zhitao Guan, Jing Li, Longfei Wu, Yue Zhang, Jun Wu, and Xiaojiang Du," Achieving Efficient and Secure Data Acquisition forCloud-Supported Internet of Things in Smart Grid" IEEE internet of things journal,vol. 4, no. 6, december 2017

[13] Dr Shekha Chenthara,Khandakar Ahmed,Frank Whittaker 2019 "Security and Privacy-preserving Challenges of e-Health Solutions in Cloud Computing" DOI 10.1109/ACCESS.2019.2919982, © 2019 IEEE Access

[14] Arfatul Mowla Shuvo,d Md. Salauddin Amin,d Promila Haqu "Storage Efficient Data Security Model for Distributed Cloud Storage"2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC) | 978-1-7281-1110-0/20/$31.00 ©2020 IEEE | DOI: 10.1109/R10-HTC49770.2020.935696

[15] Kavya K ,Smt. Kavitha M 2020 "Military Message Passing using Consortium Blockchain Technology" Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020)IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1

Cite this article as :

T Santosh, P Cefhora, T Chandana, "Untraceable Group Data Sharing for Secure Cloud", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 5, pp. 311-316, September-October 2022.
Journal URL : https://ijsrset.com/IJSRSET229640