A Collaborative Approach to Cloud-Based Functional Packaging: Sharing Intelligence Data Securely

Kondragunta Rama Krishnaiah, Professor, Department of Computer Science and Engineering, R K College of Engineering, Vijayawada - 521456, Andhra Pradesh, India, email: kondraguntark@gmail.com

Alahari Hanumant Prasad, Professor, Department of Computer Science and Engineering, R K College of Engineering, Vijayawada - 521456, Andhra Pradesh, India, email: hanuma.alahari@gmail.com

Abstract

In cloud data sharing, ensuring security and privacy for shared files is of utmost importance. However, this becomes a challenging task, especially in an environment where membership changes frequently, and when dealing with untrusted clouds that may be susceptible to collusion attacks. To address these issues, we have developed a protected multi-proprietor data sharing plan for element bunches in the cloud. The plan incorporates AES encryption, allowing any cloud client to securely share data with others. This approach not only ensures security from untrusted users but also allows group members to split and access data securely from the cloud. Our proposal minimizes storage overhead and encryption algorithm costs, making it a practical and efficient solution for a large number of users. We've designed a secure data sharing method for dynamic members, facilitating secure key distribution without the need for a secure communication approach. Instead, users can obtain their security keys securely from the group manager. The data sharing process in our system involves multiple levels of security for a multi-owner scenario. Initially, the user selects a text-based password (OTP), which is automatically generated and sent to their corresponding email account. Upon completion of the authentication and key generation process, the shared data is encrypted using a secure algorithm. By employing these concepts, our system ensures scalability and flexibility in sharing data within the cloud environment.

Index Terms: Cloud computing, broadcast encryption, cryptography, security, group key, verification. Anti-collusion, group manager, group user

1. Introduction

Cloud computing represents the cutting-edge paradigm of computer usage in the present generation. It offers a novel approach where scalable and secure virtualized resources are provided as services over the Internet. Among the plethora of services provided by cloud providers, data storage stands out as a crucial application [1]. Many companies bring their staff together in the same cloud environment to store and access files, but this convenience also poses a significant risk to the confidentiality of sensitive data. While users trust the cloud servers maintained by the providers, the stored files may contain efficient and confidential information, such as business models. To safeguard data security, a fundamental solution is to encrypt the data files before uploading them to the cloud, ensuring that only authorized users possess the necessary decryption keys [2]. This way, unauthorized users or even server administrators cannot access the contents of the encrypted files without the proper keys [3]. Furthermore, an efficient member revocation system can be implemented to manage access control without necessitating the update of the secret keys for the remaining users, thus minimizing the complexity of key management. Security receipts are generated after every member revocation, reducing the need for multiple copies of encrypted files, and helping to minimize computational costs [4]. Addressing privacy concerns in cloud computing involves establishing a well-defined set of control models and policies that govern the monitoring and management of data, rules, and security of information and infrastructure linked with cloud computing applications [5]. Numerous procedures have been proposed to validate newly shared data [6]. However, it is worth noting that most existing work focuses on verifying the integrity of data shared by single owners, rather than considering multi-

proprietor information. Multi-proprietor data entails information that is modified by multiple users [7].

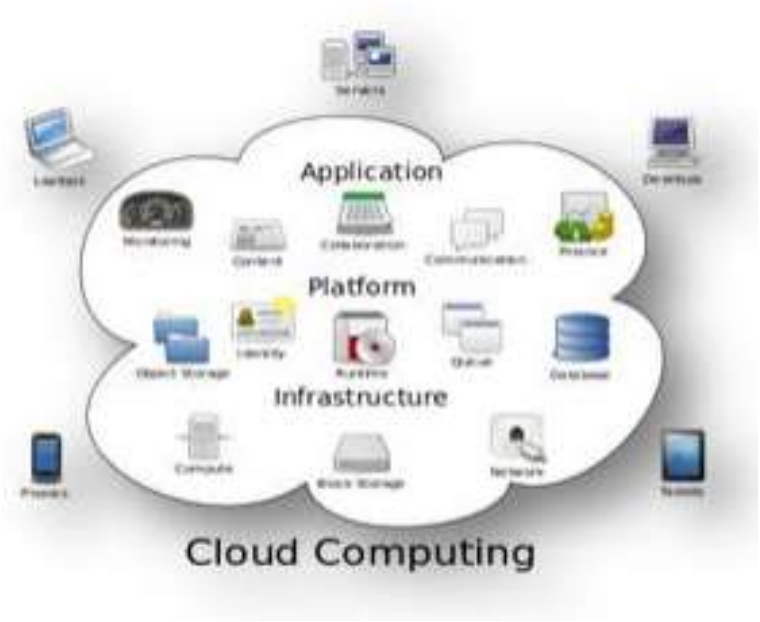

Fig. 1 Cloud Computing Model

2. Related Work

S. Kamara [9] is proposed a security for customers to store and share their security data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. The locations operation is main performance killer in the cryptographic access control system. E. Goh [8] presented a SiRiUS, a secure file system designed to be layered over in secure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key modifications and remove the simple with minimal out-of-band communication. [10] Presented cryptographic storage system that enable secure data sharing. In this methods dividing file into the file group and security each file group with a file block key. In this method at the time of user revocation the file block key uses to be updated and shared to the user the system had a heavy key distribution overhead [11] Propose secure multi owner data sharing model named as Mona. He claimed his method achieve fine grained access control and revoked user is access the shared data again after he was revoked by the cloud and revoked user this model should be suffer from the collusion attack. Revoked users use his security key to decrypt the encrypted data after his revocation. In 2003, Kallahalla [12] It enables the secure file sharing on the un trusted cloud servers uses the cryptographic storage system the files are divided into the file groups and security both groups with a unique file block key. Now the user to share the file groups with the others by delivering the matching lock box keys. The lock box key is used for modifying the file-block keys. But this changes heavy key dispersion for the enormous amounts of file sharing.

3. System Architecture

The main Objective of 2 Level Security system is same and an esoteric study of using OTP and implementation of extremely secured models employing 2 levels of security.

Level 1: Security at level 1 has been imposed by simple text-based password.

Level 2: After the successful clearance of the above level the Level 2 Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his email id. Secure environments security their resources against unauthorized access by enforcing access control model. So it increasing security is

an issue text based passwords is enough to counter such problems. Using the instant messaging service available in internet user will change the One Time Password (OTP) after image authentication. This OTP is used by user to access their personal accounts. In this paper one time password to achieve high level of security in authenticating the user over the internet.

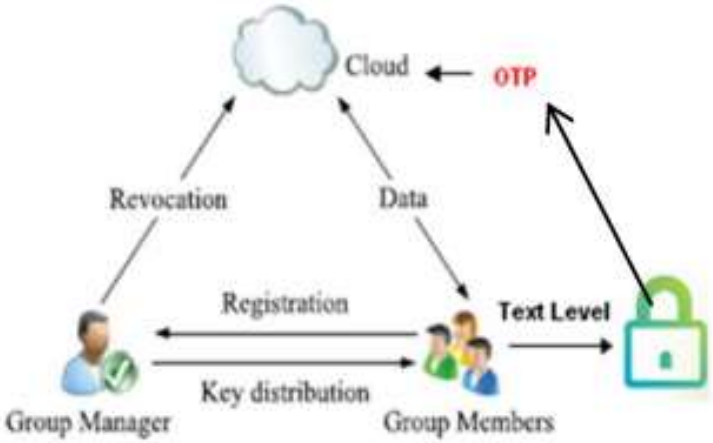

Fig. 2 System Architecture

3. Proposed System

The gathering chief will keep up the renouncement rundown of the different ways. On the off chance that any of the part leaves to gathering the part detail to added rundown and the client won't have the capacity to security login to that gathering. The new part is added to the gathering security key is given to the part. The documents which are transferred present in encoded structure and the records can be seen by gathering part as they have the authentic key.

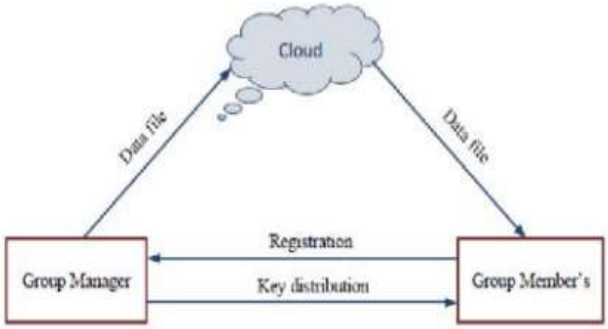

Fig. 3 Proposed systems Architecture

3.1 AES Encryption

The information 16 byte Plain data can be changed over into 4×4 square lattice.

The AES Encryption comprises of four distinct stages they are

Substitute Bytes: Uses a S-box to play out a byte-by- byte substitution of the square

Shift Rows: A Simple Permutation

Blend Columns: A substitution that makes utilization of number juggling

Include Round Key: A Simple Bitwise XOR of the present piece with the segment of the extended key (security key).

3.2 AES Decryption

The Decryption calculation makes utilization of the key in the opposite request. It may the decoding calculation is not indistinguishable to the encryption calculation.

Admin or Group Owner

1. **Group Creation** Groups are creating by admin. A company accesses its staffs in the same group to store and share files in the cloud. Any member in a group is able to fully enjoy the data storing and sharing produces provided by the cloud in the multiple-owner manner.

2. **User Registration** For the registration of user with security identity ID the group manager randomly selects a number and characters for generate random key is used for group signature generation and file decryption.

3. **Group Access Control** When a data shared occurs the tracing operation is performed by the group manager to find the real identity of the data owner. The requirement of access control is twofold. First group members is to use the cloud locations for data operations. Second unauthorized users cannot access the cloud resource at any time and removed users will be incapable of using the cloud again once they are removed.

4. **File Deletion** File stored in the cloud is deleted by either the group manager data owner. To delete a file ID data the group manager computes a signature ID data and sends the signature many ID data to the cloud.

5. **Revoke User** User revocation is performed by the group manager in a public available revocation list RL, based on which group members is encrypt their data files and security the confidentiality against the revoked users.

6. **OTP (One Time Password)** OTPs is removed number of shortcomings the associated with traditional passwords. The most important shortcoming that is addressed by OTPs is that in contrast to static passwords is not vulnerable to replay attacks.

Generation of OTP Value algorithm can be described in 3 steps:

Algorithm 1: Generation of OTP value

Step 1: Generate the HMAC-SHA value Let HMK = HMAC-SHA(Key, T) // HMK is a 20-byte string

Step 2: Generate a hex code of the HMK. HexHMK=ToHex (HMK)

Step 3: Extract the 8-digit OTP value from the string OTP = Truncate (HexHMK) the Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

Repudiate client from the gathering user renouncement is performed by gathering chief by executing a polynomial capacity done by gathering director alone. Once the client is denied from the gathering, then the gathering part is capable access the cloud assets and its information

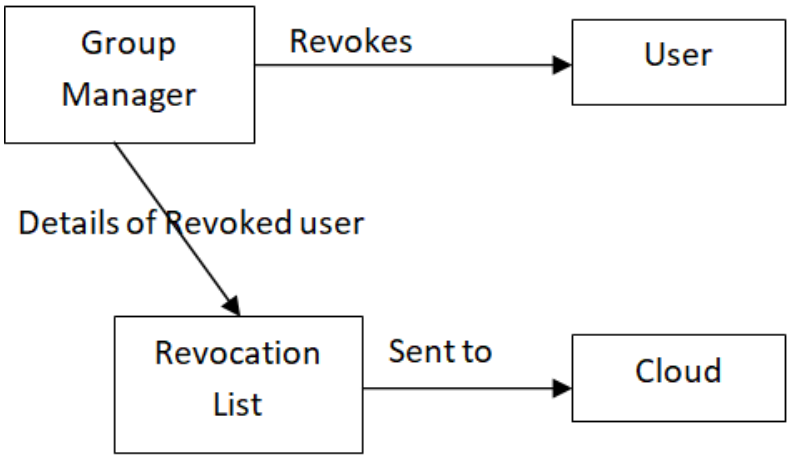

Fig. 4 Group Revocation in Cloud

4 Results And Discussion

Number of group member is store and destitute data files with others in the group by the cloud . User revocation is achieved without involving the remaining users and signed receipts will be collected after secure content sharing. The remaining users is used to update security preserved data sharing for dynamic groups in the cloud the method combines the group signature and signed receipt and dynamic broadcast encryption method. Specially, the group signature and signed receipt scheme enables users to anonymously use the cloud location, and the dynamic broadcast encryption model access data owners to securely share their data files with other including new joining users.

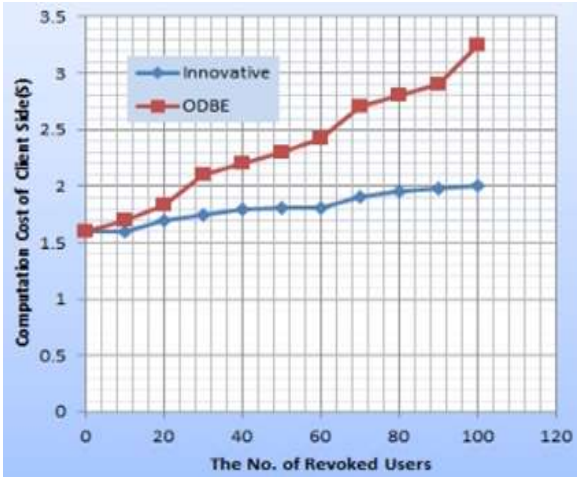

Fig. 5 ODBE Represent Model

5 Conclusion

This scheme designs a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In this scheme, the users can securely obtain their private keys from group manager without any Certificate Authorities and secure communication channels. Our scheme is support dynamic groups efficiently new user joins in the group or a user is revoked from the group the security keys of the other users do not need to be recomputed and updated. The cloud server contains all information within format of cipher and if any group member wants the particular file retrieves. We can provide more security of shared data and low cost this system is users friendly. Tempest attack and Brute-force attack at the client side though 3-Level Security system is a time consuming models it will take to strong security where we need to store and maintain crucial and confidential data secure such systems provide a secure channel of communication between the communicating entities

6 Future Work

The revoked users can not be able to get the original data files once they are revoked even if they conspire with the unfrosted cloud. In this plan we uses sending instrument in which transferring client has power to forward his information to the next client and asked for client downloading client will take for data to the transferring client.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. “A View of Cloud Computing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing,” Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, “Deduplication in cloud storage using side channels in cloud services,” Oct 2008.

[4] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[5] Zhongma Zhu and Rui Jiang, "A secure anti-collusion data sharing scheme for dynamic groups in the cloud", IEEE Transactions on parallel and distributed systems, vol.27, no.1, January 2016

[6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int‟lCryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[7] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[8] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[9] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int‟l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[11] Varun and Vamsee Mohan.B," An Efficient Secure Multi Owner Data Sharing for Dynamic Groups in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.3 Issue.6, June- 2014, pg. 730-734

[12] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.