ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Effective Data Sharing in Cloud Using Aggregate Key and Digital Signature

G. Suganyadevi[1] S. PunithaDevi[2]

P.G. Student, Department of Computer Engineering, P.A College of Engineering and Technology, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Engineering, P.A College of Engineering and Technology, Tamil Nadu India[2]

ABSTRACT: Cloud storage is storage of online data in cloud that is accessible from multiple resources. Cloud storage can provide good accessibility and reliability, towards the data stored in cloud. In cloud storage data sharing is one of the important functionality. In Key Aggregate Cryptosystem, the novelty is that one can aggregate a set of secret keys and make it as a single key, but that single key posses the power of all the keys being aggregated. All the files stored in the cloud need to be in an encrypted format for that Advanced Encryption Standard is used for encryption and decryption. The aggregate key is used for decrypting the set of cipher text. The owner of the data to be shared can release a constant-size aggregate key for decryption of cipher text set in cloud storage, but the other files stored outside the set cannot be accessed. Digital Signature is also implemented with Key Aggregate Cryptosystem to provide integrity for data stored in cloud.

KEYWORDS: Cloud storage, Aggregate key, Data sharing, encryption, decryption and Digital Signature.

I. INTRODUCTION

Cloud storage is very popular storage system. Cloud storage is storing of data to the physical storage which is maintained by third party. Cloud storage is saving of users data in logical pool and physical storage spans multiple servers that are managed by third party. Third party is responsible for maintaining the data available and accessible and physical environment should be protected and running at all time. Instead of storing data the user data in their own hard drive or any other local storage, the user can save the data to remote storage which is accessible from anywhere and any place. It reduces efforts of carrying physical storage to everywhere. By using cloud storage we can access information from any computer through internet which omitted limitation of accessing information from same computer where it is stored.

In Cloud Storage data sharing is an important functionality. For example, bloggers can allow their friends to view a subset of their private pictures. An organization may grant their employees to access a portion of sensitive data. The challenging problem in cloud is how to effectively share the encrypted data. Of course the cloud users can able to download the encrypted data that are stored in cloud and can decrypt them, then send that to others for sharing, but the problem is, it loses the value of cloud storage. Users should be able to provide the access rights for sharing data to others so that they can access these data from the server directly. However, finding an effective and secure method to share data in cloud storage is very difficult.

Recent studies focused on how to securely store and access the datas in cloud. S.G. Akl and P.D. Taylor work on the paper Cryptographic Solution to a Problem of Access Control in a Hierarchy that used the method called Partial Ordered Set (poset) [1]. The concept is all the data are stored in hierarchical manner to provide reliable and secure access to all the data. The advantage is that it provides protection not only to the files stored in memory but also for messages that are broadcast on network. The problem is time versus storage trade off in the sense the packets that occupies more space requires less time to access because it is at first place in hierarchy but packets that are in small size are at last in the hierarchy so take more time to access them.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

G.C. Chick and S.E. Tavares start his work on Flexible Access Control with Master Keys and it tried to give reliable access control to users data that are stored and transmitted across the network. For achieve reliable access use the method called Master keys based on modular exponentiation [9]. The scheme can provide large services by only using small storage space and creates fixed overhead per user, also provides hierarchal organization and expansion of set of services. The obvious application of this scheme is file storage. The key management problem is avoided by using single master secret key. The problem in using master secret keys is that since the central authority is managing the master secret key it may sometimes leads to leverage of master secret key.

W.G. Tzeng works on cryptographic key assignment problem to assign cryptographic keys to set of partial ordered set so that the cryptographic key of higher order classes can be used to derive the cryptographic key of lower class [21]. For this it uses a new method called time bound cryptographic key assignment scheme. The cryptographic keys of a class are different for each time period. There is central authority (CA) that generates and assigns keys to each class in the hierarchy. All secret parameters are processed and managed by CA. The advantage is that even if the key is lost, unauthorized person cannot decrypt the data since it uses different keys of a class for each time period. The number of public parameters is independent of total number of classes in the hierarchy. The drawback in time bound key assignment scheme is it requires large number of keys to be generated.

D. Boneh et al works on Aggregate and Verifiably Encrypted Signatures from Bilinear Maps that generate Aggregate signatures for messages. The purpose is to verify the integrity and confidentiality of those messages. The aggregate signatures are generated using bilinear mapping algorithm. The main advantage of using aggregate signatures is introducing the size of chains and communication bandwidth because aggregate signatures are of single constant size. The problem of using aggregate signature is construction of signature requires extra structures provided by bilinear maps.
Y. Sun and K.J.R. Liu starts their works on Scalable Hierarchical Access Control in Secure Group Communications. It uses the method of Multi group key management scheme to present a multi-group key management scheme that achieves a hierarchical access control by employing an integrated key graph and by managing group keys for all users with various access privileges [20]. The advantage in this scheme is to provide hierarchical access control in group communication. This scheme is suitable for both centralized and contributory environments. In Centralized key management, depends on a centralized server, called as the key distribution center (KDC) that generates and distributes encryption keys. The contributory key management schemes do not rely on centralized servers. Every group member makes can contribute independently and participates in the process of group key establishment. The drawback in this scheme is group applications contain more data streams and require the mechanism to manage more complicated access control policy.

Michael Brenner et al. work on the concept of improving the security in cloud computing and it uses homomorphic encryption for improve the data security in cloud. A growing number of compute and data storage jobs are performed on remote resources. In a cloud environment the customer cannot be sure about the location in that a particular job is physically executed and thus cannot rely on the security and confidentiality of the remote resource. A solution for this problem is operating on encrypted functions and encrypted data. The method is to compute a secret program on an untrusted resource using fully homomorphic encrypted circuits and it helps to improve the security of data.

S.S.M. Chow et al started their work on cloud computing and developed the paper called Simple Privacy-Preserving Identity-Management for Cloud environment SPICE. Cloud computing has been envisioned as the next generation architecture of IT enterprise it provides on demand self service, ubiquitous network access and location independent resource pooling. It uses group signatures in order to preserve the identity of the user. The Cloud users can make use of service providers to allocate enough storage space and manage it properly. The problem is that the privacy and security becomes critical.

II. KEY AGGREGATION

The main motivation of the proposed work is to provide secure data storage and improved data sharing in cloud. In the new system aggregate keys are used to improve the data sharing in cloud. The data integrity is a main thing to be considered in cloud. The system also provides the integrity towards the data stored in cloud.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

In key aggregate cryptosystem it provides a new method to improve the data sharing in cloud. The novelty is that one can aggregate a set of secret keys and make it as a single aggregate key. This single aggregate key will be used to decrypt the set of message [11].

All the files stored in cloud should be in encrypted format. The AES algorithm will be used to encrypt and decrypt the files in order to store them in cloud. All the files are stored in cloud storage and whenever needed the user can access it from the cloud. Since all the personal files are stored, the security should be provided to files stored in cloud. In key aggregate cryptosystem the main idea is to improve the data sharing by improving the security when files are shared among the cloud users.

In Key Aggregate Cryptosystem the novelty is that one can aggregate a set of secret keys and make it as a single aggregate key. The owner of the key can release this single key to anyone who wants to access the data stored in cloud. Instead of sharing multiple keys, the user can send single key to share multiple files.

In Setup Phase the data owner executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter.

The KeyGen Phase is executed by data owner to generate the public or the master key pair (pk, msk). The key needed to encrypt and decrypt the files are generated.

The Encrypt Phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m), the encryption algorithm takes input as public parameters pk and a message m. The algorithm encrypts message m and produces a ciphertext C such that only a user that has a corresponding key only able to decrypt the ciphertext C.

- Input= public key pk, message m
- Output = ciphertext C.

The Fig 1 describes the architecture of key Aggregate Cryptosystem.

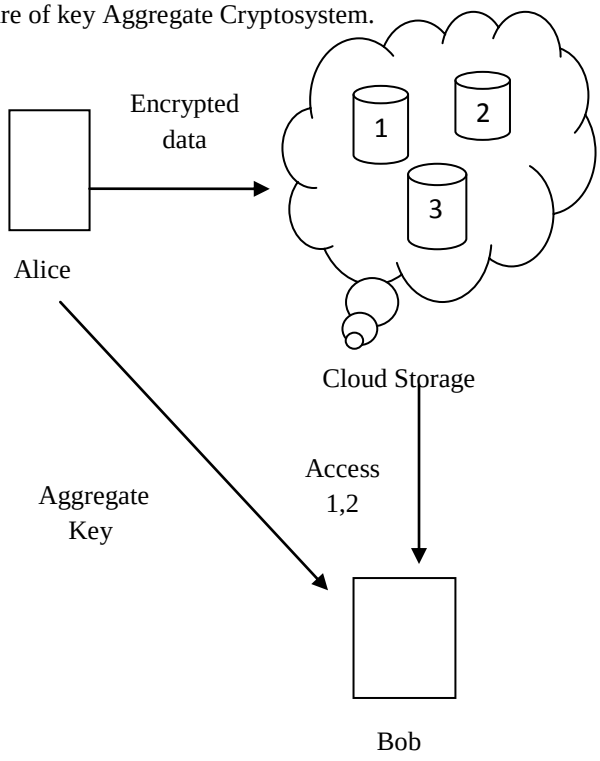

Fig 1 Architecture of Key Aggregate Cryptosystem

The Extract Phase is executed by the data owner to provide the decryption rights for a certain set of ciphertext classes to a other cloud users.

1. Input = secret key k.
2. Outputs= aggregate key denoted by k_S.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

The Decrypt Phase is executed by the candidate those have the decryption authorities. Decrypt (kS, S, i, C), the decryption algorithm will takes the input as key k, and a ciphertext C, i denotes the ciphertext in the set S.

1. Input = k_S and the set S
2. Outputs = m if i element of S

It takes the set of messages to be decrypted and apply the corresponding aggregate key to decrypt the files and produce the decrypted files as output.

III. DIGITAL SIGNATURE

In Key Aggregate Cryptosystem it mainly concentrates on effective data sharing in cloud. The Key Aggregate Cryptosystem also considers the integrity of data that are stored in cloud. To provide integrity towards the user data the digital signature is used.

Digital Signature is a process that guarantees that the contents of a message have not been altered. Digital signatures rely on certain types of encryption to ensure authentication. Authentication is the method of verifying that information is coming from a trusted source [19]. Digital signatures employ a type of asymmetric cryptography. The Key Aggregate Cryptosystem uses the RSA signing algorithm to generate the digital signature.

The RSA public-key algorithm actually uses two different keys called the public key and the private key. The private key is known only to its owner, while the public key can be available to anyone. In Public-key algorithms two keys are used in that one key is used for encryption, the other is necessary for decryption. In digital signatures, the private key generates the signature, and the corresponding public key validates that signature. The RSA algorithm alone cannot be used to sign the document so that hashing algorithm is also used along with that.

1. A one-way hash of the document is produced using SHA algorithm.
2. The hash is encrypted with the private key of the RSA there by signing the document.
3. The document and the signed hash are transmitted.
4. The recipient produces a one-way hash of the document.
5. Using the RSA algorithm, the recipient decrypts the signed hash with the sender's public key.

If the signed hash matches the recipients hash, the user can know that the signature is valid and the document is intact. Using the digital signature method the cloud users can verify the integrity of the stored data in cloud.

IV. EVALUTION AND RESULTS

The Key Aggregate Cryptosystem allows the users to upload files, share their files and to download and access the files. Uploading files into cloud requires all the files need to be encrypted and then stored. The Fig 2 shows the uploading of files into cloud

Fig 2 Upload the files to cloud

Sharing files among cloud users is done by using the aggregate key. The files are downloaded from cloud and then decrypted for accessing the files. Fig 3 describes the sharing of data to other cloud users.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

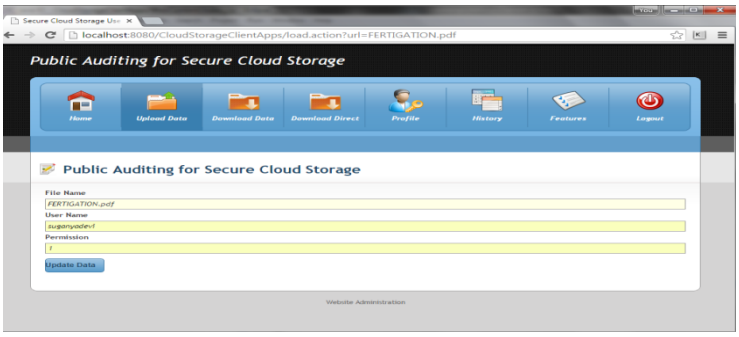

Fig 3 Data sharing

The owner of the data can set the permissions to access the shared data. Digital Signature allows the users to verify the integrity of the data by generating and verifying the signature at the time data storage and retrieval. The Third Party Auditors will perform the signature generation and verification. The Fig 4 describes the signature generation.

Fig 4Signature Generation

The integrity of data the can be checked whenever needed. The Fig 5 describes the signature verification.

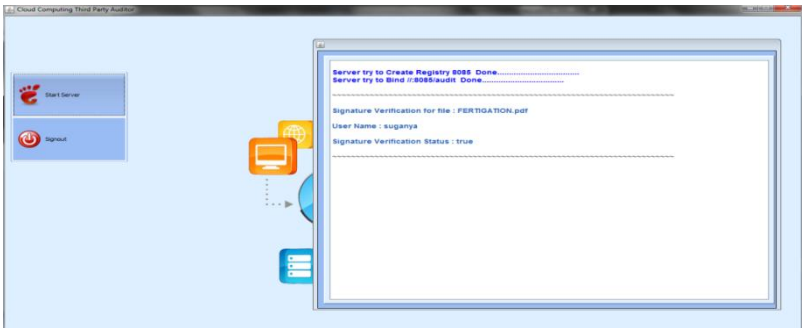

Fig5 Signature Verification

All the actions performed by the cloud users can be seen through the server log messages.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

V. CONCLUSION

To share data flexibly is a important role in cloud computing. Users prefer to upload their data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Key Aggregate Cryptosystems provides delegation of secret keys for different files stored in cloud storage in the form of single aggregate key. The proposed work additionally includes digital signature to provide integrity towards the users data.

REFERENCES

1. Akl S. G. and Taylor P. D. (1983), 'Cryptographic Solution to a Problem of Access Control in a Hierarchy', ACM Trans. Computer Systems, vol. 1, no. 3, pp. 239-248.
2. Atallah M. J., Blanton M., Fazio N. and Frikken K. B. (2009), 'Dynamic and Efficient Key Management for Access Hierarchies', ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43.
3. Benaloh J. (2009a), 'Key Compression and Its Application to Digital Fingerprinting', technical report, Microsoft Research.
4. Benaloh J., Chase M., Horvitz E. and Lauter K. (2009b) 'Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records', Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114.
5. Boneh D. and Franklin M. K. (2001), 'Identity-Based Encryption from the Weil Pairing', Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229.
6. Boneh D., Gentry C., Lynn B. and Shacham H. (2003), 'Aggregate and Verifiably Encrypted Signatures from Bilinear Maps', Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432.
7. Bowers K. D., Juels A., and Oprea A. (2009), "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198.
8. Chase M. and Chow S. S. M. (2009c), 'Improving Privacy and Security in Multi-Authority Attribute-Based Encryption', Proc. ACM Conf. Computer and Comm. Security, pp. 121-130.
9. Chick G. C. and Tavares S. E. (1989), 'Flexible Access Control with Master Keys', Proc. Advances in Cryptology (CRYPTO '89), vol. 435, pp. 316-322.
10. Chow S. S. M., Chu C. K., Huang X., Zhou J., and Deng R. H. (2012), 'Dynamic Secure Cloud Storage with Provenance', Cryptography and Security, pp. 442-464, Springer.
11. Chow S. S. M and Deng H. (2014), 'Key Aggregate Cryptosystem for scalable data sharing in cloud storage', IEEE Trans. Parallel and Distributed systems, vol. 25, no. 2 pp. 468-477.
12. Chow S. S. M., He Y. J., Hui L. C. K. and Yiu S. M. (2012a), 'SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment', Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543.
13. Goyal V., Pandey O., Sahai A., and Waters B. (2006), 'Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data', Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98.
14. Guo F. Mu Y., Chen Z. and Xu L. (2007), 'Multi-Identity Single-Key Decryption without Random Oracles', Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398.
15. Guo F., Mu Y. and Chen Z. (2007a), 'Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key', Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575, pp. 392-406.
16. K. Ren, C. Wang, and Wang Q.(2012), "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73.
17. Sahai A. and Waters B. (2005), 'Fuzzy Identity-Based Encryption', Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473.
18. Sandhu R. (1988), 'Cryptographic Implementation of a Tree Hierarchy for Access Control', Information Processing Letters, vol. 27, no. 2, pp. 95-98.
19. Sowparnika M., Dheenadayalu R. (2013), 'Improving data integrity on cloud storage services', International Journal of Engineering Science Invention., Volume 2 pp. 49-5, Feb.
20. Sun Y. and Liu K. J. R. (2004), 'Scalable Hierarchical Access Control in Secure Group Communications', Proc. IEEE INFOCOM '04.
21. Tzeng W. G. (2002), 'A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy', IEEE Trans. Knowledge and Data Eng., vol. 14, no. 1, pp. 182-188, Jan./Feb.
22. Wang B., Chow S. S. M., Li M., and Li H. (2013), 'Storing Shared Data on the Cloud via Security-Mediator', Proc. IEEE 33rd Int'l Conf.Distributed Computing Systems (ICDCS).
23. Wang C., Chow S. S. M., Wang Q., Ren K., and Lou W. (2013a), 'Privacy- Preserving Public Auditing for Secure Cloud Storage', IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb.