A Review on Deduplications of encrypted data using Attribute-Based Encryption on Cloud

Harshal Shriram Deshpande[1], Miss Manjiri Karande[2]

[1] *student M.E. (Second year), Computer Science &Engineering Department, Pdm.Dr.V.B.Kolte College Of Engineering, Malkapur, Maharashtra, India*

[2] *Asst professor, Computer Science &Engineering Department, Pdm.Dr.V.B.Kolte College Of Engineering, Malkapur, Maharashtra, India*

ABSTRACT

Attribute-based encryption (ABE) can be used to share some specific vulnerable data or credential which was used in cloud computing while providing services.Whereas,the standard ABE system provide this security by avoiding de duplication of credentials for forming identical data in all terms. And in this paper, to make it possible we create private cloud to find out the duplication of data which consume the storage of duplicates data.We tried to present an attribute-based storage system in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage. Compared with the prior data deduplication systems, this system has two advantages. In addition, we put forth a methodology to modify a cipher text over one access policy into cipher texts of the same plaintext but under other access policies without revealing the underlying plaintext.

Keyword: -Attribute based encryption, deduplication, cloud, hybrid cloud, semantic

1. INTRODUCTION

For protection of data from handling misused we make use of attribute based encryption. Our work in this area is based on Attribute based Encryption. It is one of the techniques that are more suitable for storing data with encryption. While sharing of data system provide Data confidentiality, Fine grained access control, Removing Key escrow problem, Removing Revocation problem, Scalability Cloud contains large amount of data stored in it, hence retrieving the correct information plays a very important role. The indexing of document collection is performed by Lucene Privacy and security are the important issues in cloud computing. In the existing system KGC is not separated from master admin, hence master admin knows both keys that generated from KGC so in the absence of user master admin may access the private data. This problem is overcome in the proposed system as KGC is separated from the master admin. [2]

2. LITERATURE SURVEY

In Junbeom Hur proposed a novel CP-ABE scheme for a secure data sharing system. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol between the KGC and the data storing center with their own master secrets. But the limitation of this system was reliability and load balancing under real time environment. In [3], author proposed a novel CP-ABE scheme is used to solve the key escrow problem by escrow free key issuing protocol generated by using two party computations. Fine-grained user revocation per each attribute could be done by proxy encryption. They have done survey based on existing Attribute based encryption schemes and their implementation which gives an idea that there are still limitations in existing system also these approaches gives idea about more scope in encryption techniques.

In the authors presented comparative study of different attribute based encryption schemes like KP-ABE,CP-ABE, ABE with nonmonotonic access structure, HABE,MABE based on various parameters suggest that these schemes are classified according to their access policy and after analyzing these schemes we found that the main access policies are KP-ABE and CP-ABE and further policies are derived using either of these policies as a base and found that cipher text policy based ABE schemes are more efficient and scalable to securely manage user data in the data sharing system. In author introduced a new Cryptograhic construct called Blind Storage and implemented it using a novel, light weight protocol Scatter Store. Also showed how a dynamic SSE scheme can be constructed using Blind Storage.[3]

3. EXISTING SYSTEM

In this system 2PC protocol is used and the encryption is done with the help of the two keys generated. The plaintext entered by the data owner is encrypted partially by the public key which resides with the master admin and the other partial half is done with the help of the private key which resides with the data owner. The 2PC protocol works on SSL handshake which is a technique used to manage the encryption keys during the plaintext encryption done by both the keys. Similarly, the decryption of data is done by the private key from the admin and the public key from the user. Key escrow is not fully resolved in this system which dealt with key revocation.[4]

4. PROPOSED SYSTEM

Proposed system provide some privacy mechanism to protect the data and shared in cloud and avoid de duplication of credentials in cloud to avail maximum storage.Toimprove the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager to reveal the identity of the signer based on verification metadata in some special situations.[5]

Description Of AES

The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of cipher text. Each round consist of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.[5][6]

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
   - AddRoundKey—each byte of the state is combined with the round key using bitwise xor
3. Rounds
   - SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
   - ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
   - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey
5. Final Round (no MixColumns)
   - SubBytes
   - ShiftRows
   - AddRoundKey
6. Key Expansion—round keys are derived from the cipher key using Rijndael's key schedule
7. Initial Round
   - AddRoundKey—each byte of the state is combined with the round key using bitwise xor
8. Rounds
   - SubBytes—a non-linear substitution step where each byte is replaced with another according to alookup table.Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
   - MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
9. AddRoundKey
10. Final Round (no MixColumns)
    - SubBytes
    - Shift Rows
    - AddRoundKey

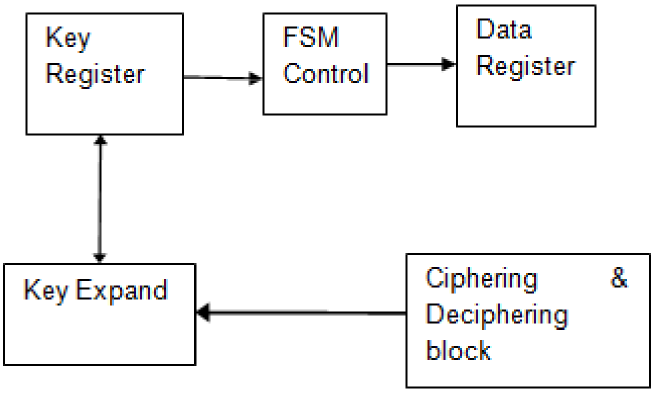

Fig 1: Block Diagram of the Privacy preserving public auditing architecture

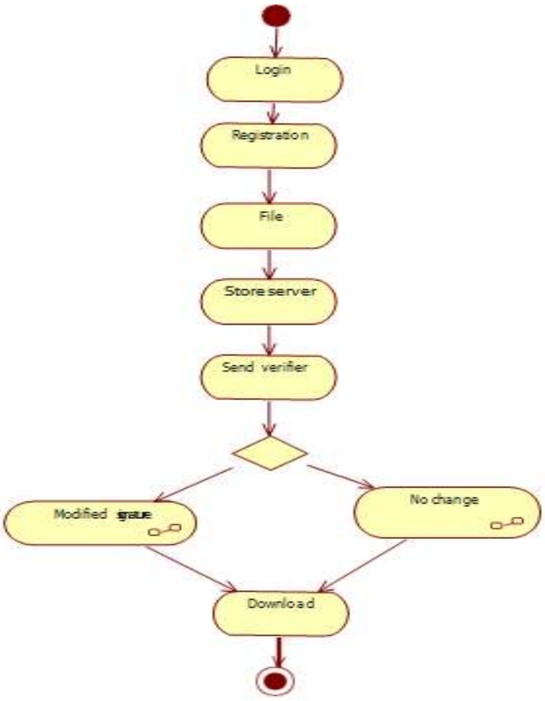

Fig. 2: Activity Diagram of Privacy Preserving Public auditing system

In fig 2, as we proposed for the verification of metadata by using AES algorithm and implement it the process of registration by new user is essential. Once the user has registered with the system the file uploading mechanism started by verifying it in proper utilization by generating a proper signature through rig signature concept. registered user pretend to use the uploaded file the signature
When another shared if modified then the second user can't able to download the file and if there is no modification with signature and completely authenticate then the file downloads with no issue[7][8][9]

5. CONCLUSION

Hence an attribute-based storage system with secure deduplication in a hybrid cloud setting, where a private cloud is responsible for duplicate detection and a public cloud manages the storage.Eventhough the technology is available to provide proper authentication but fail to provide accuracy in that regards. Also Comparing with the prior data deduplication systems, this system provided some advantages which can be used to confidentially share data with users by specifying access policies rather than sharing decryption keys. Also we achieved the standard notion of semantic security for data confidentiality while existing systems only achieve it by defining a weaker security notion. We make the system more efficient in terms of its data accuracy and timing parameters and keep a scope of modification in that regards.

6. FUTURE SCOPE

An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.[10]

7. ACKNOWLEDGEMENT

I express deep gratitude for enthusiasm and valuable suggestions that I got from my guide Miss. Manjiri Karande, Asst. Professor of Computer science & Engineering Department for successful completion of this paper. This was not possible without her invaluable guidance. I pay deep regards to our HOD Prof .Y. B. Jadhao Principal Mr. A. W.Kharche who are instrumental in setting standards for the students to achieve.

8. REFERENCES

[1] JunbeomHur "*Improving Security and Efficiency in Attribute-Based Data Sharing*", VOL. 25, NO. 10, Addagada, Sridevi "*Indexing and Searching Document Collections using Lucene*" (2007) University of New Orleans Theses and Dissertations. Paper 1070

[2] Apurva Gomase1, Prof. Vikrant Chole "*A Review on Secure System Implementation using Attribute Based Encryption*" IJCSMC, Vol. 3, Issue. 11, November 2014, pg.465 – 468

[3] Mangesh Gosavi1 , Tabassum Maktum2 "*Survey of Various Attribute Based Encryption Schemes Used in Data Sharing System*" IJARCSSE, 2015

[4] Michael O’Keeffe “*The Paillier Cryptosystem*” By The College of New Jersey Mathematics Department April 18, 2008

[5] D. Kavitha, S. Hemavathy “*A Survey on Cloud Computing Security Issues And Multi-Keyword Ranked Data Search Efficiency in Blind Storage*” Vol. 3, Issue 9, September 2015

[6] Keerthi B, V Rajesh kannan “*Implementation of Attribute Hiding Strategy and Key Revocation in Cloud Environment*”IJISET Vol. 1 Issue 2, April 2014.

[7] Muhammad Naved,ManojPrabhakarn, carl A.Gunter ”*Dynamin Searchable Encryption Via Blind Storage*” Univercity of Illinois at Urbana-Champaign

[8] Changsha Ma ; Chang Wen Chen “*Secure media sharing in the cloud:Two-dimensional- scalable access control and comprehensive key management*”, Multimedia and Expo (ICME), 2014 IEEE International Conference, DOI: 10.1109 /ICME. 2014. 6890308, Publication Year: 2014 , Page(s): 1 -6

[10] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "*Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application", Proc. Int'l Workshop Information Security Applications (WISA '09)*, pp. 309-323, 2009.