ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

A Survey on Scalable and Secure Data Sharing in Cloud Storage Using KAC

Pooja BhanudasVarale[1], PayalRajendra Bhongale[2], Kavita Tatyaba Kad[3], Prajkta Kumar Potekar[4], Prof. Gunaware N.G[5].

UG Student, Department of Computer Engineering, Hon. Shri. Babanrao Pachpute Vichardhara Trust's Pa^{r}ikrama College of Engineering, Kashti, Savitibai Phule Pune University, Pune, Maharashtra, India[1,2,3,4]

Assistant Professor, Department of Computer Engineering, Hon. Shri. Babanrao Pachpute Vichardhara Trust's Parikrama College of Engineering, Kashti, Savitibai Phule Pune University, Pune, Maharashtra, India[5]

ABSTRACT: With the advent of cloud computing, it has become increasingly accepted fordata owners to outsource their data to public cloud servers while allowing datausers to retrieve this data. For privacy concerns, secure searches over encryptedcloud data have aggravated several research facilities under the single owner model.We describe newpublic-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher textsare feasible. The novelty is that one can aggregate any set of secret keys andmake them as compact asa single key, but encompassing the power of all the keysbeing aggregated. In other words, the secret key holder can release a constantsizeaggregate key for flexible choices of cipher text set in cloud storage, but theother encrypted files outside the set remain confidential. This compact aggregatekey can be easily sent to others or be stored in a smart card with verylimited secure storage. We provide formal security analysis of our schemes in thestandard model. We also describe other application of our schemes. In particular,our schemes give the first public-key patient-controlled encryption for flexible hierarchy, which was yet to be known.

KEYWORDS: Cloud storage, data sharing, key-aggregate encryption,patient-controlled encryption

I.INTRODUCTION

Cloud storage is gaining popularity recently. In enterprise settings, we see the rise in demand for data outsourcing, which assists in the strategic management of corporate data. It is also used as a core technology after many online services for personal applications. Networks, it is easy to apply for free accounts for email, photo album, file sharing and/or remote access, withstorage size more than 25GB (or a few dollars for more than 1TB). Together with the current wireless technology, users can access almost all of their files and emails by a mobile phone in any area of the world.

II.RELATED WORK

This section introduces existing related work and describes their similarities and differences from our work.

A. PRIVACY PRESERVING RANKED MULTI-KEYWORD SEARCH FOR MULTIPLE DATA OWNERS IN CLOUD COMPUTING:

With the advent of cloud computing, it has become increasingly popular for data owners to outsource their data to public cloud servers while allowing data users to retrieve this data. For privacy concerns, secure searches more than encrypted cloud data have motivated several research works under the single owner model. However, most cloud servers in practice do not just serve one owner; instead, they support several owners to share the benefits brought by cloud computing. In this paper, we propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM).

Disadvantages:
They only give the assurance to security for users that fulfil all their searches at once.We notice this limitation by introducing stronger definition that guarantees security even when users execute more realistic searches.

B. ANALYSIS GIVE GUIDANCE TO THE CHOICE THE SIZE OF CIPHER TEXT SPACE:

At the end suggest a unique and efficient transformation that can be applied to any OPE scheme. Our deep study shows that the transformation yields a scheme with more result safety in that the scheme contest the one-wayness and window one-wayness attacks.

C. PRIVACY PRESERVING PUBLIC AUDITING FOR SECURE CLOUD STORAGE:

Enabling public auditability for cloud storage is of critical importance so that users can
resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free.

Disadvantage:
However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources.

D. SECURE CONJUNCTIVE KEYWORD SEARCH OVER ENCRYPTED DATA:

A security model for conjunctive keyword search over encrypted data and present the first schemes for conducting such searches securely. We propose first a scheme for which the communication cost is linear in the number of documents, but that cost can be incurred " earlier than the conjunctive query is asked. The security of this scheme relies on the Decisional Diffie-Hellman (DDH) assumption.

Disadvantage:
In order to retrieve documents satisfying a certain search standard, the user gives the server a capability that allows the server to identify exactly those documents.

III.PROPOSED ALGORITHM

Input: C_i = Encrypt (pk, i, mi)
It is executed by data owner and for message m and index i, it computes the
ciphertext as C.
Ci : Cypher Text. pk : Public key. i : index . mi: Message.
Output: Downloaded file.
AES Algorithm:

- AES is a block cipher with 128 bits block length.
- AES allows for 3 different key lengths: 128, 192, or 256 bits. Our discussionprimarily will assume that the key length is 128 bits.item Encryption is going to be 10 rounds of processing for 128 bit keys, 12rounds for 192 bit keys and 14 rounds for 256 bit keys.
- All the remaining rounds are identical with exception for the last round ineach case in Computer and Network Security.
- One single-byte based substitution step is include in each round of processing,a row-wise permutation step, a column-wise mixing step, and the addition of the round key. These four steps executing order is different forencryption and decryption.item To enhance the processing steps used in a single round, it is best tothink of a 128-bit block as consisting of a 4 4 matrix of bytes, arranged.
- Therefore, the first four bytes of a 128-bit input block will occupy the firstcolumn in the 4 4 matrix of bytes. The next four bytes occupy the secondcolumn, thus it will continue.
- The 4X4 matrix of bytes is referred to as the state array.
- AES also has the perception of a word. A word consists of 4 bytes means32 bits. Hence each column of the state array is a word, as is each row.
- Each processing round works on the input state array and produces an output state array.
- The output state array produced by the last round is rearranged into a 128-bit output block.

- Unlike DES, the decryption algorithm differ largely from the encryption algorithm. Somehow the same steps are used in encryption and decryption,the order in which the steps are carried out is different, as mention previously.
- AES, notified by NIST as a standard in 2001, is a slight variation of the Rijndael cipher invented by Belgian cryptographers Vincent Rijmen, Joan Daemen.
- Whereas the block size that AES requires at 128 bits, the original Rijndaelcipher works with any block size (and as well any key size) that is a multipleof 32 as long as it will exceeds 128. The state array for the different block size still has only 4 rows in the Rijndael cipher. But the number of columns depends on size of the block. For instance, when the block size is 192, the Rijndael cipher requires a state array to consist of 4 rows and 6 columns.

IV. SYSTEM ARCHITECHTURE

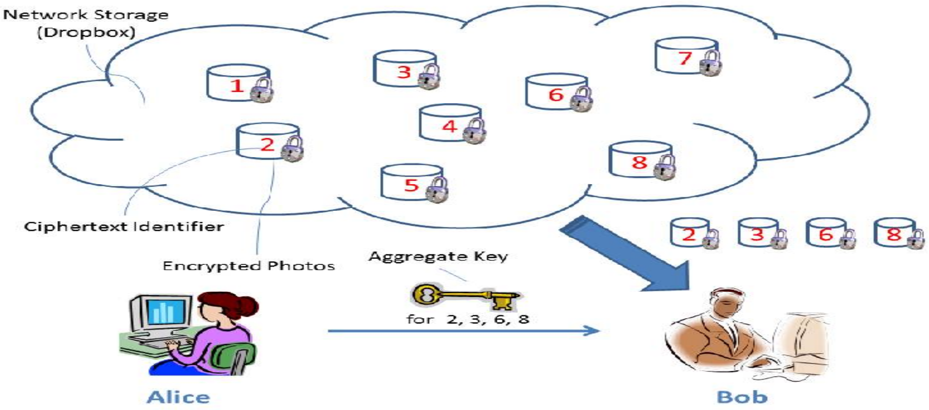

Fig.1 Alice shares files with identifiers 2, 3, 6 and 8 withBob by sending him a single aggregate key

“To design an efficient public-key encryption scheme whichsupports flexible delegation in the sense that any subset of theciphertexts (produced by the encryption scheme) is decryptableby a constant-size decryption key (generated by the owner ofthe master-secret key).”

V. CONCLUSION AND FUTURE WORK

In this paper, we discussed the public-key encryption method for protecting the privacy of data from the attackers who may obtain the data by legal or other means, data stored by users and secret information. The main aim of this approach is to obtain the aggregate key of constant size empowered with the decryption rights for the number of files is possible by the valid user. Along with the privacy of data, the secrecy is also preserved by encrypting the user data before dumping into the cloud. Protection of the users’ data privacy in cloud storage is an important aspect. With the help of mathematical tools, the encryption schemes are becoming more flexible and have started involving many encryption and decryption keys for a single application. But this project introduced the unique concept of the aggregation of the keys involved in decryption process. The cost of storing and transmitting the ciphertexts is lower as they are constant-sized. This compact aggregate key can be conveniently sent to others or be stored in a smart card with very limited secure storage. It is modelled in such a way keeping different security levels and extensions. Storing the delegated keys in the mobile devices which have no trusted software, there is a possibility that the key gets disclose. So designing a leakage-proof cryptosystem which supports flexible and efficient key delegation is an interesting direction. In this project, the AES algorithm is used for encrypting the files. A more secured and efficient algorithm can be used in future so as to cope up with the speed and for security purpose.

REFERENCES

1. Cheng-Kang Chu ,Chow, S.S.M, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng , ―Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage ‖, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.
2. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ―Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,‖ in Procee dings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
3. J. Benaloh, ―Key Compression and Its Application to Digital Fingerprinting, ‖Microsoft Research, Tech. Rep., 2009.
4. B. Alomair and R. Poovendran, ―Information Theoretically Secure Encryption with Almost Free Authentication, ‖ J. UCS, vol. 15, no. 15, pp. 2937 –2956, 2009.
5. D. Boneh and M. K. Franklin, ―Identity -Based Encryption from the Weil Pairing, ‖ in Proceedings of Advances in Cryptology –CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.
6. A. Sahai and B. Waters, ―Fuzzy Identity -Based Encryption, ‖in Proceedings of Advances in Cryptology -EUROCRYPT '05, er. LNCS, vol. 3494. Springer, 2005, pp. 457–473.
7. S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters, ―Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions,‖ in ACM Conference on Computer and Communications Security, 2010, pp. 152–161.
8. F. Guo, Y. Mu, and Z.Chen, ―Identity-Based Encryption:How to Decrypt Multiple Ciphertexts Using a Single Decryption Key,‖ in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer, 2007, pp. 392–406.
9. F. Guo, Y. Mu, Z. Chen, and L. Xu, ―Multi-Identity Single-Key Decryption without Random Oracles,‖ in Proceedings of Information Security and Cryptology (Inscrypt '07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384 –398.
10. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y (2010) Fine-grained data access control systems with user accountability in cloud computing. IEEE second international conference on cloud computing technology and science(CloudCom) 2010, pp 89–96.

BIOGRAPHY

Pooja Bhanudas Varale Pursuing the Bachelor Degree in Computer Engineering from H.S.B.P.V.T.COE,Kashtiunder SPPU, Pune

Payal Rajendra Bhongale Pursuing the Bachelor Degree in Computer Engineering from H.S.B.P.V.T.COE,Kashtiunder SPPU, Pune

Kavita Tatyaba Kad Pursuing the Bachelor Degree in Computer Engineering from H.S.B.P.V.T.COE,Kashtiunder SPPU, Pune

Prajkta Kumar Potekar Pursuing the Bachelor Degree in Computer Engineering from H.S.B.P.V.T.COE,Kashtiunder SPPU, Pune

Prof. Gunaware N.G. is working as an Assistant Professor in Computer Engineering Department from H.S.B.P.V.T.Parikrama College of Engineering, Kashtiunder Savitribai Phule Pune University,Pune.He received Master of Technology (M.Tech.) degree in 2016 from RGPV, Bhopal, MP, India. His research interests are Cloud Computing (Pervasive Computing), Smart Systems Design etc.