Cryptosystem for Scalable Sharing of Data Using Single key Versus N keys

Ms. Monali S. Bachhav Prof. Amol Potgantwar

Abstract - **Sharing of the data is an important functionality in cloud storage. In this article the total concentration is on how confidentially, efficiently and flexibly the information share with other in cloud storage. Here the description of thenew public-key cryptosystem which generates fixed-size ciphertexts such that efficient delegation of decryption rights for any set of cipher texts are possible. The innovation is that one can aggregate any set of the secret keys and make them as compact as a one key, but encompassing the power of all keys being aggregated. The secret key owner can create fix size aggregate key for variable options of encrypted text set in cloud storage, but remaining files from the set are confidential .The aggregate or cumulative key can suitably sent to others or stored in smart card with less secure storage. Appropriate security investigation of this approach is given in standard model. Public-key patient-controlled encryption structure yet to be known.**

Keywords - **Data sharing, patient controlled encryption, cloud storage, key-aggregate encryption**

.

I.INTRODUCTION

Cloud storage is gaining popularity recently. Cloud storage is a model in which data is maintained, controlled and back up remotely and made accessible to users over a network. It is also used as a core technology behind many online services for personal applications.

Nowadays, it is simple to apply for free accounts for email, file sharing and/or remote access, with storage capacity more than 25GB. Confidentiality of the data , a traditional way to assure is to depend on the server to access control after authentication, which means that illegal privilege will expose the whole data. In sharing nature or tendency cloud computing surrounding, things are more worse. Information from different client can be hosted on the single virtual machine but reside on the single physical machine. Data from virtual machine can be easily get to another VM co-resident with target one. Cloud users do not have confidence that cloud server can keep their information secure. Sharing information is main task of cloud. The most critical issue is how the encrypted data is share securely. Users can download encrypted data from the storage , decrypt them and then send it to others for sharing purpose, but it decreases value of the cloud storage. Users should be able to delegate access rights of the data sharing to others so that they can access these data from the server directly. Encryption comes in two ways-Symmetric key or asymmetric key.

In today's cryptography, a fundamental issue we often study is about leveraging the secrecy of small piece of knowledge into ability to perform cryptographic functions multiple times.

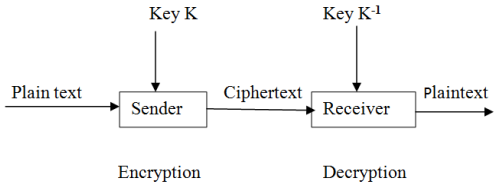

Fig1.Cryptography

II.LITERATURE REVIEW

In 1976 Whitfield Diffie and Martine E. Hellman [1], two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing. In [2] Selim G. Akl and Peter D.Taylor A scheme based on cryptography is proposed for access control in a system where hierarchy is represented by a partially ordered set (or poset). Straightforward implementation of the scheme requires users highly placed in the hierarchy to store a large number of cryptographic keys. A time versus- storage trade-off is then described for addressing this key management problem.

In [3] Ravindrapal S. Sandhu proposed a cryptographic implementation is proposed for access control in situation where users and information items are classified into security classes organized as a rooted tree, with most privileged security class at root. In [4] Gerald C. Chick,. Stafford E. Tavares how to create a master key scheme for controlling access to a set of services. Each master key is a concise representation for a list of service keys, such that only service keys in this list can be computed easily from the master key. Our scheme is more flexible than others, permitring hierarchical organization and expansion of the set of services. In [5] Chung Kei Wong group key management service, using any of the three rekeying strategies, is scalable to large groups with frequent joins and leaves. In particular, the average measured processing time per join/leave increases linearly with the logarithm of group size.

In [6] Dan Boneh proposed a new identity-based encryption based on weil pairing. In [7] Fuh-Gwo presents efficient key

assignment scheme based on the one way hash function.This scheme ensures that any user can't decrypt data longer with his expired secret key.Sandro Rafaeli presents a group key management which was divided into three main classes: centralized group key management protocols,decentralized architecture and distributed key management protocols [8]. In [9] Kin-Ching Chan,.S.-H. Gary Chan present a number of the proposed key management schemes for data confidentiality. categorize these schemes into four groups: key tree-based approaches, contributory key agreement schemes supported by the Diffie-Hellman algorithm, computational number theoretic approaches, and secure multicast framework approaches. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps [10] proposed Security model for aggregate signature which are useful for reducing size of the certificate chains and for reducing message size.In [11] Qiong Zhang, Yuke Wang Key management scheme for hierarchical access control which consider both partially order user relations and patially order data stream relations. Also proposed algorithm for constructing a logical key graph which is suitable even when users and data streams have complex relations. In [12] A multi-group key management scheme that manages keys for all members with different access privileges which reduces communication, computation and storage overhead associated with key management. Leonardo B. Oliveira, Diego F. Aranha, Eduardo Morais [13], present TinyTate, the first known implementation of pairings for sensor nodes based on the 8- bit/7.3828-MHz ATmega128L microcontroller (e.g., MICA2 and MICAz motes). New re-encryption schemes [13] that realize a stronger notion of security and demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system [14] in which some security issues created. Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci how three malicious users can handle public and private information to misuse their tamper-resistant devices in order to compute some encryption keys that they should not be able to learn [15]. Fuzzy Identity Based Encryption, which allows for error-tolerance between the identity of a private key and the public key used to encrypt a ciphertext. Security of these scheme proved under Selective-ID model [16].Dan Boneh, Xavier Boyen, Eu-Jin Goh Identity Based Encryption (HIBE) system where the cipher text consists of just three group elements and decryption requires only two bilinear map computations, regardless of the hierarchy depth[17].

In [18] drawback is Selectively shared only at a coarse-grained level i.e. giving private key to another party to avoid this presents a a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE).Matthew Green, Giuseppe Ateniese problem of Identity-Based proxy re-encryption, where cipher texts are transformed from one identity to another to overcome these Enabling non-interactive, unidirectional proxy re-encryption in the IBE[20].CCA-secure unidirectional PRE scheme.A security-mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners introduces by Boyang Wang, Sherman S. M. Chow, Ming Li using multi signer model in [21].

III. Overview Of System Model

A. Existing System

In the existing system if there are n files ,then n keys are required for the encryption and decryption purpose. So that the network traffic increases. The sender of the data or key requires the storage space for the n keys. At same time the receiver also requires the storage space more. For the decryption purpose it requires the more number of iteration. Difficult for mapping the files and key from the receiver side. As shown in figure there are 8 files and each require the single key if we share the file1, file2, file3, file6 then receiver requires the 4 keys key1,key2,key3,key6.

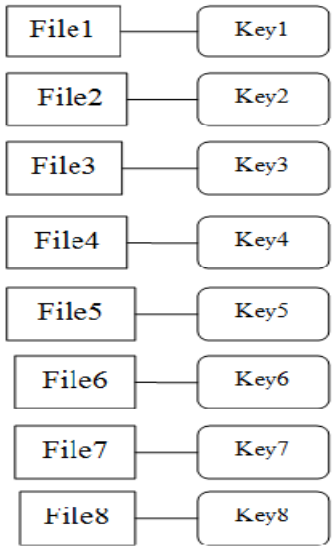

Fig. 2. Multiple Files Multiple Keys

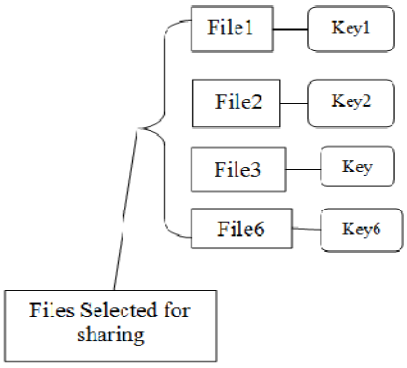

Fig3. Files for sharing

B. Proposed System

In the proposed system if there are n files, then single aggregate key is required.

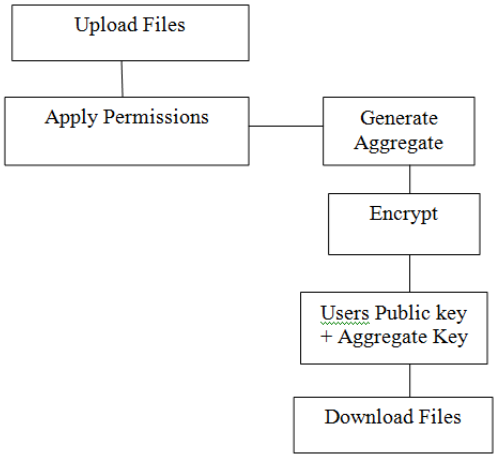

Fig. 4 System Architecture

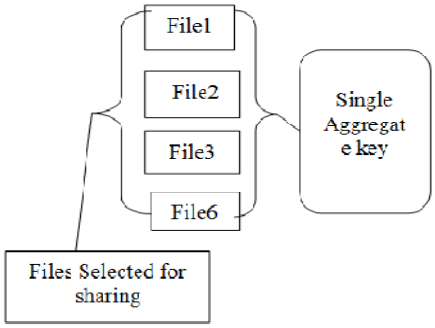

Fig.5 Multiple Files One Key

C.Aggregate Key Generation Algorithm

1. First Setup Data
2. All the key like k1,k2 ,k3 are in string format then it will converted into bytes using Byte Encoder.
3. Then every string converted in string to number like,
K1=12356
K2=56423
K3=35641
4. All set key combine then it can give separator for that different key like,12356 0 56423 0 35641 here no value consider as separator.
5. secrete key i.e, S.
6. key convolution : we are use the quadratic equation, f(x)=(n1x + n2x + S)
here the x is consider as 2 or any number.
7. Display String format of key.

IV. Performance Analysis

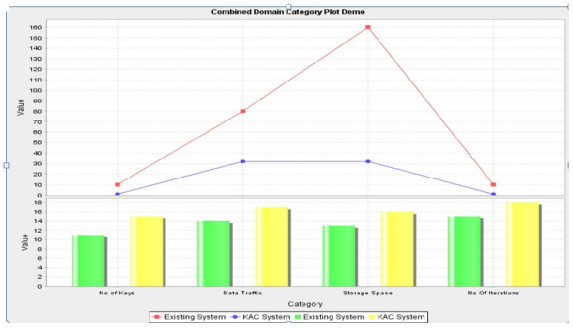

Fig.6 Graph shows analysis of sharing 10 Files By Both Files

Our approaches allow the compression factor F (F =n in our schemes) to be a tunnable parameter, at the cost of O(n)-sized system parameter. For the encryption constant time is required, while decryption can be done in O(jSj) group multiplications (or point addition on elliptic curves) with 2 pairing operations, where S is the set of classes of ciphertext decryptable by the granted aggregate key. As expected, key extraction requires O(jSj) group multiplications as well, which seems inescapable. However, as verified by the experiment results, we do not need to set a very high n to have better compression than the tree based approach. Note that group multiplication is a very fast operation. The execution times of Setup, KeyGen, and Encrypt are independent of the delegation ratio r. In our experiments, KeyGen takes 3:3 ms and Encrypt takes 6:8 ms.As expected, the running time complexities of Extract and Decrypt increase linearly with the delegation ratio r (which determines the size of the delegated set S). timing results also conform to what can be seen from the equation in Extract and Decrypt two pairing operations take negligible time, the execution time of Decrypt is roughly a double of Extract.We remark that for applications where the number of ciphertext classes is large but the non-confidential storage space is limited, one should setup our schemes using the Type-D pairing bundled with the PBC, which only require 170-bit to represent an element in G. For n = 216, the system parameter requires approximately 2:6 megabytes, which is as large as a lower quality MP3 file or a higher-resolution JPEG file that a typical cell phone can store more than a dozen of them. We saved expensive secure storage space without the hassle of managing a hierarchy of delegation classes.

Our approach is more flexible than existing system. Encryption can be done in the constant time while for the decryption purpose aggregate key and users private number is used which send through e-mail.

The aggregate key which is used for decryption purpose is dynamically created for the each user which is having the varying size. Our decryption time is less than the existing approach.The proposed system requires less storage space network traffic and key as compared to the existing system.

V. Conclusion

In cloud privacy of the users information is main question. With huge mathematical tools, cryptographic schemes are getting more flexible and involve multiple keys for a single application. In this article, we focus on providing security to the user using aggregate key and private number. Our approach is more flexible than the existing. The key size is dynamically varying.

On the other side when individual carries delegated keys around mobile device without particular accurate hardware, the key is prompt to escape, designing a leakage resilient cryptosystem [27] allows competent and flexible key delegation is interesting way.

ACKNOWLEDGMENT

The authors would like to acknowledge Computer Engineering department, SITRC and all the people who provided with the facilities being required and conductive conditions for completion of the paper.

REFERENCES

[1]. White field Diffie and Martin E. Hellman "New Directions in Cryptography" IEEE Transactions on Information Theory, vol. It-22 No.6, Nov. 1976

[2] S. G. Akl and P. D. Taylor, "Cryptographic Solution to a Problem of Access Control in a Hierarchy," ACM Transactions on Computer Systems (TOCS), vol. 1, no. 3, 1983,pp. 239-248.

[3] R. S. Sandhu, "Cryptographic Implementation of a Tree Hierarchy for Access Control," Information Processing Letters, vol. 27, no. 2, 1988, pp. 95-98.

[4] G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in Proceedings of Advances in Cryptology - CRYPTO89, ser. LNCS, vol. 435. Springer, 1989, pp. 316-322.

[5] Chung Kei Wong, "Secure Group Communications Using Key Graphs" IEEE/ACM Transactions on networking, vol. 8, no. 1,Febru- ary 2000

[6] D. Boneh and M. K. Franklin, "Identity-Based Encryption from theWeil Pairing," in Proceedings of Advances in Cryptology – CRYPTO 01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213-229.

[7] Fuh-Gwo Jeng, Xiao-Wei Huang "An Efficient Key Assignment Scheme with Time-Bound Constraints for Hierarchical Access Control," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, 2002, pp. 182-188.

[8] Sandro Rafaeli, David Hutchison "A Survey of Key Management for Secure Group Communication" ACM Computing Surveys, Vol. 35, No. 3, 2003,pp. 309-329.

[9] Kin-Ching Chan, S.-H. Gary Chan," Key Management Approaches to Offer Data Confidentiality for Secure Multicast" IEEE Network, 2003.

[10] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT 03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416-432.

[11] Qiong Zhang,Yuke Wang,Jason P. Jue "Hierarchical Access Control in Group Communication"International Journal of Network Security, Vol.7, No.3, Nov. 2008, pp.323-334.

[12] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," IEEE INFOCOM, 2004

[13] Leonardo B. Oliveira, Diego F. Aranha, "TinyTate: Computing the Tate Pairing in Resource-Constrained Sensor Nodes," in Pro- ceedings of Advances in Cryptology - CRYPTO 05, ser. LNCS, vol. 3621. Springer, 2005, pp. 258-275

[14] Giuseppe Ateniese, Kevin Fu"Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage", journal version has been accepted for publication in ACM Transactions on Information and System Security (TISSEC), February 2005.

[15] Alfredo De Santis, Anna Lisa Ferrara, Barbara Masucci " Enforcing the security of a time-bound hierarchical key assignment scheme" Elsvier Inc. 6 July 2005.

[16] A. Sahai and B. Waters, Fuzzy Identity-Based Encryption, in Proceedings of Advances in Cryptology - EUROCRYPT 05, ser. LNCS, vol. 3494. Springer, 2005, pp. 457-473.

[17] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," in Proceedings of Ad- vances in Cryptology - EUROCRYPT 05, ser. LNCS, vol. 3494.Springer, 2005, pp. 440-456.

[18] V. Goyal, O. Pandey, A. Sahai, and B.Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 06). ACM, 2006, pp. 89-98.

[19] Matthew Green, Giuseppe Ateniese, "Identity-Based Proxy Re-Encryption" , 2007.

[20] R. Canetti and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re-Encryption," in Proceedings of the 14th ACM Conference onComputer and Cmmunications Security (CCS 07). ACM, 2007, pp.185-194.

[21]Cheng-Kang Chu,Sherman S.M.Chow,Wen-Guey Tzeng, Jianying Zhou,and Robert H. Deng, Senior Member,IEEE ,"Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage"IEEE Transaction on Parallel And Distributed System.Volume:25,2014

AUTHOR'S PROFILE

Author's Name : Monali S. Bachhav is a P.G. student of Computer Engineering at SITRC College of Engineering , Nasik under Savitribai Phule Pune University . She has completed her undergraduate Course of engineering from Savitribai Phule Pune University. Her areas of interest include Cloud Computing.

Author's Name : Prof. Amol Potgantwar is a Asst. Professor of the Department of Computer Engineering, Sandip Foundation's, Sandip Institute of Technology and Research Centre, Nashik, Maharashtra, India. The focus of his research in the last decade has been to explore problems at Near Field Communication and it's various application In particular, he is interested in applications of Mobile computing, wireless technology, near field communication, Image Processing and Parallel Computing. He has register patents like Indoor Localization System for Mobile Device Using RFID & Wireless Technology , RFID Based Vehicle Identification System And Access Control Into Parking, A Standalone RFID And NFC Based Healthcare System. He has recently completed a book entitled Artificial Intelligence, Operating System, Intelligent System. He has been an active scientific collaborator with ESDS, Carrot Technology, Techno vision and Research Lab including NVIDIA CUDA, USA. He is a member of CSI, ISTE, IACSIT .