Cryptosystem for Scalable Sharing Of Data Using Aggregate Key-A Review

Ms. Monali S. Bachhav **Prof. Amol Potgantwar**

Abstract — **A cryptosystem is pair of algorithms that take a key and convert plaintext to ciphertext and back. Information distribution is main functionality in cloud storage. In this article the total concentration is on how confidentially, professionally and easily the information share with other in cloud storage. The secret key holder 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.**

Key Words — **Data sharing, patient controlled encryption, cloud storage, key-aggregate encryption**

I. Introduction

Cryptosystem is a pair of algorithm that take a key and convert plaintext to ciphertext and back. Cryptosystem is combination of three elements: keying information, operational procedure & encryption engine for the secure use.

Cloud storage is a service where data is remotely maintain, managed and backup. Cloud storage is currently very popular. In enterprise we see demand of outsourcing of information. It is used as basic technology for very online services for private applications. In cloud computing things become worse due to share-tendancy. Privacy of data rely on the server to force access control after authentication which cause many times unexpected expose of the information. Information from different users can collected on seprate virtual machines but reside on single physical machine. Information from virtual machine can be easily get to another VM co-resident with target one. Cloud users do not have guarantee that cloud server can keep their information secure.

Sharing information is main task of cloud. For example, bloggers can want their personal photo , organization grant permission for this personal data. But problem is sharing of the encrypted data and effectiveness of that task. Take another example of dropbox for explanation. Alice can collect personal picture on dropbox and she thinks no one can watch her photos. Due data loss possibility Alice does not feel secure and she encrypts all picture using own key before uploading. Another day her friend wants all pictures of the year in which bob appear. Alice use share option of dropbox but problem is that how to delegate decryption rights to bob.

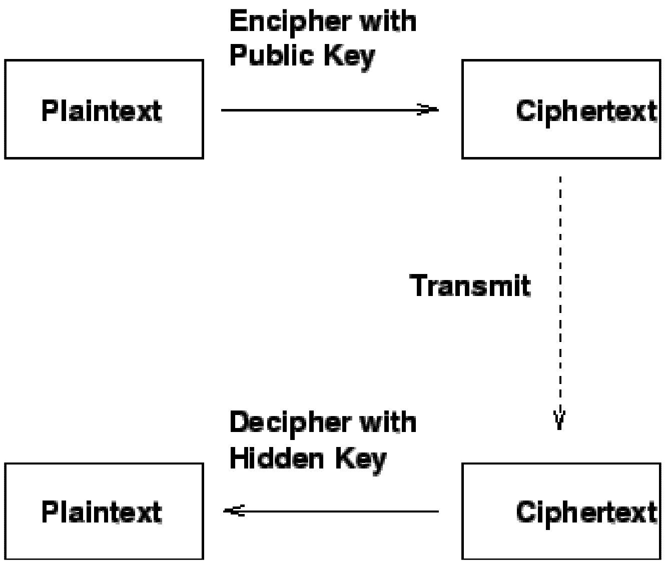

Fig. 1. Cryptosystem

Then there are 2 critical ways

1.Alice encrypt whole picture with one encryption key and give secret key to bob.

2.Encrypt all picture with special key and send corresponding secret key to bob.

The first way is not secure because data is leake to bob. For another way practical issue of the efficiency. There are many key as many as number of pictures are shared. Transmission of the keys requires secure channel and storing requires secure storage.The prize and problems involve generally increase with number of decryption keys to be share. It is very expensive.Encryption comes in two flavor-symmetric or asymmetric key.

Therefore, best solution is that Alice encrypt pictures with distinct public key ,but but only sends one decryption key.

Since, the decrypted key send via proper channel and kapt private, limited size key is always desirable.The current research mainly concentrate on reducing communication requirements like aggregate signature.

In current cryptography t problem we generally observe is secrecy of small part of knowledge into the capability to perform cryptographic functions. We know how to raise more commanding decryption key in the way that it allows it allow various ciphertext , without increasing its size. For solving this problem another public-key encryption call key-aggregate cryptosystem is introduce. In this message encrypt under not only a public key but identifier of encrypted text called class. Owner of key holds master-secret key for various classes. The extraction key have aggregate key which compact than secret key.

With our solution, Alice can easily send bob a single aggregate key via secure electronic media. Bob download that encrypted pictures and use this aggregate key to decrypt the pictures the scenario is depicted in fig.2.

The range of the encrypted text, master key,public-master key and aggregate key in KAC scheme are fix size. The public system parameter has linear size in ciphertext classes, but only small portion needed each time and it can be access on demand from huge cloud storage.

A.Key Aggregate Encryption

These technique consist of five polynomial-time algorithm.

1. Setup: executed by data holder to setup an account on untrusted server. The output is public system paprmeter param, which is remove from others algoritm input.
2. KeyGen: To randomly create public/master-secret key pair it is executed by the data owner
3. Encrypt: executed by any one who want encrypt data.
4. Extract: Data owner execute it and gets the aggregate key for set of the indices.
5. Decrypt: executed by delegate who receive or gat the aggregate key.

There are two functional requirements compactness and correctness or accuracy.

B. Sharing Encrypted Data

A canonical application of KAC is sharing of the data. The key aggregation feature is useful when we want allocation to be efficient and flexible. The technique enable provider of the content to share or distribute her data in secure and proper way, with constant and small ciphertext expansion, by sharing to each authorized user a single and small aggregate key. Aggregate key is used for the decryption of the message.

The data sharing idea in cloud using KAC , explained in fig.2

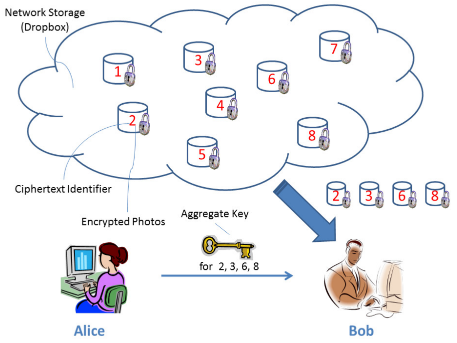

Fig. 2. Using KAC for data sharing in cloud storage

II. Related Work

First we study literature of security or cryptography. In [5],[6],[7] cryptographic key assignment scheme aim to reduce the cost in collecting and organizing secret key for general use of cryptography.By using tree structure, key for a given branch use to generate descendents nodes key. Presently permitting parent key all decendent nodes key implicitly grant. [9] Sandhu proposed technique for generating tree hierarchy of symmetric key by using iterative application of one way function. The idea generalized from tree to graph. Advanced cryptosystem kay assignment technique sypport access that can be modeled by cyclic or acyclic graph [23],[10]. Many schemes produces keys for symmetric- key cryptosystems, even many key derivations requires modular arithmetic used in the public key, which are generally more expensive than normal “symmetric key operations” such as pseudorandom functions.

In [9] Yan Sun proposed multi group key management scheme that achieves hierarchical access control with integrated key graph and muti group key management scheme. In [2] Benaloh present a encryption scheme for sharing more keys in broadcast scenario.

A.Compact Key in Identity-Based Encryption

Identity based encryption scheme in ([20], [21], [22]) is a form of the public key encryption . In this the public key of user is set as string-identity of user. In the IBE Private Key Generator which hold a master secret key and issue it to other user as per their identity. The user who encrypt the message can take public parameter and identity of user to decrypt message. The recipient decrypt ciphertext using own secret key.

Guo et al. [14], [3] tried to create IBE with key aggregation . One of their technique [14] assumes random oracle but other one not [3]. Very importantly , their aggregation of key [14],[3] comes at expense of the size for both ciphertext and public parameter. This increases cost of storing and transferring ciphertext, which is not practical in some conditions.

In fuzzy IBE [13], one individual secret key can decrypt siphertext under multiple identities which are close in more metric space, but not for random set of identities and it does not match with key aggregation idea.

B. Other Encryption Scheme

Attribute based Encryption [4], [15] allows each encrypted text to be connected with feature, and the master-secret key possesor can take out secret key for a policy of this feature so that encrypted text can be decrypted by this key if it is associated attributes conforms to policy. In ABE important issue is collusion-resistance not the compactness of secret keys. The range of the encrypted text is not fix [16].

A PRE schme permit Alice to delegate to server ability to convert ciphertext encrypted under own public-key ones bob.The Proxy Reencryption PRE technique is well known to various application [17].Using PRE scheme only shift the secure key storage requirement from delegatee to proxy. Thus it is not suitable to let proxy reside in storage server. It will not suitable so each decryption needs individual interaction with proxy.

C. Construction of KAC

Boneh et al. [18] present collusion-resistant broadcast encryption scheme by using this the basic scheme is designed. Their technique support fixed-size secret keys, each key only has

1. Encryption:- output ciphertext
2. Extract
3. Decrypt:- Output message

The decryption can be done more efficiently .

To make extended scheme best different ciphertext classes suggested for various purposes opposite to different public-keys. This key extension approach can also view as key update process. Suppose a secret ka value is compromised

Then we can replace it with new key value. The less aggregate key size reduces communication overhead for transferring the new key.

III . New Patient Controlled Encryption

Patient controlled encryption has been studied in [2]. In the PCE the health record if divided into hierarchical representation depend on the different ontologies and the patients are the parties who create and store secret key. When there is need of accessing record ,a patient will release secret key for the access of record to the healthcare. In the Benaloh et al. [2], proposed three solution.

1. Symmetric key PCE for fixed hierarchy(tree based method)
2. Public key PCE for constant hierarchy(the IBE analog of folklore method).
3. RSA based symmetric key PCE for flexible hierarchy.

Current work propose solution for omitted piece, public key PCE for flexible hierarchy , which the existence of efficient construction was an open issue.

Each patient can create her own hierarchy in fig. 3 as per her self need, or follows the set of the catagories recommended by the electronic medical record system such as xray, medications and so on. If patient wants to give access right to her doctor, she choose any subset of different categories and give a single key, from which key total categories computed. Thus, we can basically choose any hierarchy, useful when the hierarchy can be complex. Finally single healthcare deals with many patient and the data of the patient is possible to stored on the cloude because of his large size, compact size key and easy key management are of the paramount.

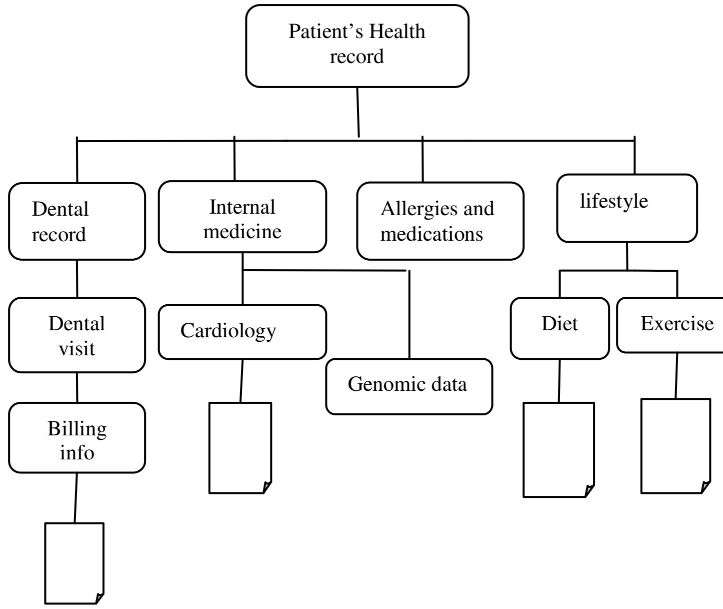

Fig. 3. Hierarchical patients health record

Conclusion

Users information privacy is a central question of cloud storage. With extra mathematical tools,cryptographic schemes are getting more flexible and involve multiple keys for a single application.In this paper,we think how to "reduce" secret keys in public-key cryptosystems which support delegation of secret keys for various encrypted classes in cloud storage. These approach is more flexible than hierarchical key assignment which simply save spaces if whole key owner distribute a similar set of privileges.

A restriction is the predefined bound of number of most ciphertext classes. In cloud stoage, number of encrypted text generally grows fastly. That's why we have to reserve more ciphertext classes for future work otherwise extend public key.

The parameter can be downloaded with encrypted text, it would be better if its size is not dependent of more number of ciphertext classes. On the other side when one carries delegated keys around mobile device without particular accurate hardware, the key is prompt to leakage, designing a leakage resilient cryptosystem[19] allows competent and flexible key delegation is interesting way.

ACKNOWLEDGEMENT

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 review paper.

REFERENCES

[1] Cheng-Kang Chu, Sherman S. M ,"Key Aggregate Cryptosystem for Scalable Data Sharing in cloud storage", IEEE Transactions on Parallel and Distributed Systems, vol. 25, issue2,2014

[2] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.

[3] 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.

[4] 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.

[5] 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.

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

[7] G. C. Chick and S. E. Tavares, "Flexible Access Control with Master Keys," in Proceedings of Advances in Cryptology – CRYPTO '89, ser. LNCS, vol. 435. Springer, 1989, pp. 316–322.

[8] W.-G. Tzeng, "A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy," IEEE Transactions on Knowledge and Data Engineering (TKDE), vol. 14, no. 1, pp. 182–188, 2002.

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

[10] Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.

[11] 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.

[12] 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.

[13] 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

[14] 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.

[15] M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

[16] T. Okamoto and K. Takashima, "Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption," in Cryptology and Network Security (CANS '11), 2011, pp. 138–159.

[17] D. Boneh, C. Gentry, and B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," in Proceedings of Advances in Cryptology - CRYPTO '05, ser. LNCS, vol. 3621. Springer, 2005, pp. 258–275.

[18] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Transactions on Information and System Security (TISSEC), vol. 9, no. 1, pp. 1–30, 2006.

[19] T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu, "Identity- Based Encryption Resilient to Continual Auxiliary Leakage," in Proceedings of Advances in Cryptology - EUROCRYPT '12, ser. LNCS, vol. 7237, 2012, pp. 117–134.

[20] Q. Zhang and Y. Wang, "A Centralized Key Management Scheme for Hierarchical Access Control," in Proceedings of IEEE Global Telecommunications Conference (GLOBECOM '04). IEEE, 2004, pp. 2067–2071.

[21] J. Benaloh, "Key Compression and Its Application to Digital Fingerprinting," Microsoft Research, Tech. Rep., 2009.

[22] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.

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**
Completed his M.Tech from VJTI Mumbai, Mumbai University in 2009. Presently he is working as HOD at SIEM & SITRC College of Engineering, Nasik, Maharashtra, India. He is handling the post of Director Journal, IRF Group, Pune. His research interest includes knowledge Discovery, Data Mining, Cognitive Radio and Wireless Communication, Image Processing.Processing, VHDL.