Access of Encrypted Personal Record in Cloud

Miss. Shwetambari G.Pundkar
Department of Computer Science and Engineering
Sant Gadge Baba Amravati University
Amravati,Maharashtra,India
shwetapundkar@gmail.com

Dr. G. R. Bamnote
Department of Computer Science and Engineering
Sant Gadge Baba Amravati University
Amravati,Maharashtra,India
grbamnote@rediffmail.com

Abstract**—** Personal record is a data, which is collected and stored in cloud computing to gain cost benefit and better access control. In maintaining Personal Record, cloud computing plays an important role, since minor organizations are not affordable to keep own servers to maintain the personal record for cost and security aims. Providing availability to various stake holders become a deadly process in isolated individual servers with encryption technology. Cloud ensures that personal record availability to the necessary user at any point of time. In any country, there is a law which governs to maintain privacy of special records, and hence maintaining recodes in cloud are subjected to privacy concerns and high risk of getting exploited. There are various encryption schemes to provide personal records security and privacy in Cloud computing. Extensive logical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Keywords*- Personal records, symmetric-key technique, cloud computing, data sharing, data security.*

*****

I. Introduction

Personal record is a model of data interchange, which stores the data at a third party, such as cloud computing. However, there have been extensive confidentiality concerns as personal data could be exposed to those third party servers and to unauthorized parties. To assure the individuals control to their own records, it is a favorable method to encrypt the records. The issues such as risks of confidentiality, scalability in key management, flexible access, and efficient user revocation, have remained the most significant experiments toward accomplishing security reason, cryptographically imposed information access control. The novel structure and devices for information access control to records stored in could servers is to achieve fine-grained and scalable data access control for records and control symmetric encryption techniques to encrypt each personal record. Different from previous works in secure data, the main focus on the multiple data owner consequence, and divide the users in the record system into multiple security domains that greatly reduces the key complexity for owners and users [1].

A high degree of individual's privacy is guaranteed by exploiting multi authority symmetric key encryption. The scheme also provides run time modification of access policies or file attributes, supports capable on-demand user to access emergency scenarios [2]. Wide-ranging analytical and experimental results are presented which show the security, scalability, and efficiency of our planned scheme. The agenda of scheme is to overcome the unique challenges by several record vendors and users, in that greatly reduce the complexity of key management which improves the privacy guarantees compared with previous works [3]. The use of symmetric key encryption for encrypting the data, so that user can allow access not only by personal way, but also by using various users from different department with different expert persons who has high qualifications, and affiliations. Likewise, improving an existing scheme to grip well-organized and on-demand user revocation, and prove its security [4].To develop the trust for the growth of cloud computing. The cloud providers must prevent the user's data from unofficial access. One technique to encrypt the data on client side before loading it in cloud storage, however this technique has too much burden from client side in terms of key management, preservation perspective etc. Other way is to keep the security service like computing hash of data and confirming integrity of data, encryption and decryption service if provided by same cloud storage, the data compromise cannot be ruled out. The Software is only in charge for encryption and decryption of data, cloud computing verifies the hash of the data and does not store any data in trusted cloud server. The encrypted information and original data are stored in Separate Cloud which is Secure, therefore even if the loading cloud system manager has access user data, since the data is encoded and it will be difficult for the system manager to understand the encrypted data. While the user takes the data from Cloud, it is decoded and then new hash is measured which is then compared with unique data which is stored in Cloud in secure manner. Finally, this software application offers the user provides the facility to store the encoded data in cloud which is encrypted and decrypted in cloud, and no single cloud service provider has access to both. Other responsibility is to trust 3rd party which reliefs the client from any kind of key management or maintenance of any key information related to data on it device, because of which it allows the client to use any browser enabled devices to access such service[3][6].There are different service's provided by cloud are as follows:

- Software as a service (SaaS)

Cloud-based is an application or software as a service (SaaS) which runs on distant computers in the cloud that are operated by others users via the Internet and, usually, a web browser.

- Platform as a service(PaaS)

Platform as a service provides a cloud-based atmosphere with all requests to support the whole life cycle of building and sending web-based applications without the cost and complexity of obtaining and managing the underlying software, hardware.

- Infrastructure as a service (Iaas)

Infrastructure as a service provides computer resources including servers such as networking, storage, and data center space.

II. Literature Review

The works was enforced to access data by attribute based encryption is done till now. To recognize access control, the traditional public key encryption based schemes either gain high key management overhead, or need encrypting multiple copies of a file using different user's keys. To improve the scalability of the above solutions, one-to-many encryption methods such as attribute encryption can be used. The data are encoded under a set of attributes so that multiple users who proper keys can decoded. This theoretically makes encryption and key management more efficient. The important property of attribute based encryption is preventing against user collusion. A number of works used attribute encryption to realize fine-grained access control for outsourced data. Especially, there has been an attribute encryption to secure electronic records. Recently, proposed a work on attribute encryption frame for electronic records systems, where each patient's e-health care records files are encoded using a transmission variant of that allows direct withdrawal. However, the cipher text produces linearly with the number of users. In a variant of attribute encryption that allows allocation of access rights is proposed for encode e-records. Cipher text rule attribute encryption to manage the sharing of personal records, and the new concept of social skilled domains is introduced. In investigated using attribute encryption to generate self-protecting e-records, which can either be kept on cloud or cell phones so that records could be opened when the health provider is off-line [1][7].

However, there are many common disadvantages of the above works. First, they assume the use of a particular trusted expert in the system. This is not only creating a load bottleneck, but also suffers from the key problem since the trusted expert can access all the encoded files. In accumulation, it is not applied to delegate all attribute controlling tasks to one trusted expert, including endorsing all users attributes and generating secret keys. In fact, dissimilar organizations usually form their own areas and become suitable experts to define and certify different sets of attributes fit in to their areas. For example, a specialized link would be responsible for verifying medical fields, while a local health provider would certify the job levels of its staffs. Second, there still absences an effective and on-demand user revocation device for attribute encryption with the support for run time policy updates modifications, which are vital parts of secure personal record sharing. Finally, most of the previous works do not distinguish between the personal and public domains, which have different attribute meanings, key management requirements, and scalability issues [6].

For efficient key sharing, classified model for planning of personal files are used. The data of the user is encoded each value, and an elements are constructed to minimize the number of keys. In this technique if the numbers of users are more than then working becomes difficult, as well as the key sharing is a big problem. Other results includes public key encryption because the user's read and write privileges are planned [10] [11].Proposed hierarchical identity based encryption which had high key organization. Even if there have been many improvements in fields of authentication and authorization using user method in the areas of media sharing and personal satisfied none of them deals with dynamic federated identity management. This scenario has provides a methodology of verification in consumer e-devices, by giving the authorizations to the user to share the content rights and facilities in secure and trusted environments, temporarily

A key difference is in a single important authority is still supposed to manage the whole expert area. Recently, key-policy attribute encryption to secure data in the cloud where a single information owner can encode data and share with multiple authorized users, by using keys that contain attribute-based privileges. They also plan a method for the data owner to repeal a user efficiently by delegating the updates of affected encoded texts and user secret keys is used in cloud server. Since the key operations can be gathered over time, their pattern achieves low amortized. However, in this scheme, the data vendor is also a trusted authority at the same time. It would be useless to be applied to a personal record system with multiple data vendors and users, because then each user would accept many keys from multiple vendors, even if the keys contain the same sets of attributes. On the other hand, a multiple-authority attribute encryption solution in which multiple users, each governing a diverse subset of the system's users attributes, generate user secret keys together. A user needs to obtain one part of key from each trusted authority [5]. Earlier, health care providers have stored medical records of their patients on paper locally. This allowed an organized atmosphere with easy management of data confidentiality and security. The growing use of private computers and modern information technology in medical organization allowed for a moderate effort to manage confidentiality of individual medical records. This was due to the dispersed and close by managed organization of each institution. Contract out leads to a difficult system where the sensitive data are stored and managed at many different places. Hence it became attractive to store and process data in the cloud. Such e-health systems assurance a more cost operational service and better service quality but the difficulty to manage data strongly and privacy rises. In commercial systems like Google Fitness, Microsoft Health Treasure house and ICW Life Device, patients store their health-related data on certain web servers called Personal Health Record (PHR). The user can track, gather, and achieve the data about their health or the status of data at on-line web sites. In contrast to personal record, which are managed by the patients, E-

Record is managed by professionals. The problems of e-records clouds are data storage and processing management of e-records infrastructure, and user experience. A secure e-records frame to ensure a vital security and confidentiality property was suggested [6]. Security in e-record systems should be imposed by encoding as well as access control. The users must be able to create and save encryption keys, so that the user's privacy is protected. But encoding would interfere with the functionality of the system. A user Controlled Encryption was planned as a result to secure and isolated storage of users records which allows the users to selectively share records [4].

Then data encoding scheme that does not needed a trusted data server was proposed. The server can implement encoded searches and updates on encoded data without knowing the plain text or the decryption keys [7]. An accessible agenda for Authorized Private Keyword Search over encoded cloud data was proposed in system [8]. With encoded data, keyword search becomes an interesting issue. In Cipher-text-Policy Attribute- Based Encryption, user's secret key is linked with a set of attributes, and the cipher-text is connected with an access structure or decoding policy over attributes. The user can decode the cipher-text if and only if the aspect set of his top-secret key contents the decoding rule specified in the cipher-text. In key rule, the encoding exerts no regulator over who has given right to entry the data, except by the choice of attributes for the data [9] [10]. Another form of CP-ABE is multi-authority CP-ABE. It allows user to encode the data according to an access rules over a set of attributes issued by two trusted authorities: the first trusted authority (TA1) of the professional domain and the second trusted authority (TA2) of the social domain (SD). The user himself takes the role of TA2. TA1 will verify users of the professional domain, and issue top-secret keys based on their attributes encoding, while the user might use the vertical of the users of the social domain to develop appropriate secret keys [11].Another system was planned to maintain e-record availability even when the sources are off-line. For this, encryption was used which helps granulated role-based and relaxed-based access control e-recode, without the need for a single, vulnerable centralized server [12]. In a multi-specialist encryption system, there will many attribute authorities, and many users [13]. To overcome the problems of, a new multi- specialist scheme was planned without a trusted specialist and with an unidentified key protocol which allows multi- specialist encryption with improved user privacy [14]. Then cipher text encryption scheme with efficient reversal was proposed. In this malicious users can be efficiently retracted .An attributes access control scheme using cipher text encryption able to attribute and user revocation capability for data was proposed. This technique had several advantages that security and scalability associated to the previous revocable cipher text encryption schemes. It allows a data owner to define the access control policy and enforce it on his outsourced data [16].

III. SECURITY ANALYSIS

The system was planned to manage Personal Records with dissimilar user access environment. The data values are planned under a cloud system. The data confidentiality and safety is assured by the system. The data attributes are selected by the personal. The information can be read by different parties. The key values are kept and distributed to the different experts. The system is boosted to support Distributed encryption model. The user's individuality based access appliance is also provided in the system. The system is divided into six major modules. They are information owner, cloud services, organization of key, security method, expert analysis and user.

Information user: This module is developed to maintain the details of record. The characteristic model is used to select complex information. User record is developed with different information collections. This assigns access authorizations to various users.

Cloud services: This module is used to store the values of the fields. The personal record information is saved in databases. User module uploads the encrypted record to the cloud. User uses the information which is maintained under cloud services.

Organization of key: This module is developing to accomplish key values for different experts. The values of keys are uploaded by the data user. Key organization process includes key insert and key deletion tasks. Dynamic rule based on key organization scheme is used in the technique.

Security Method: This module handles the encryption operations. Various encryption methods are used to encrypt the data in cloud. Using encryption technique provides a high security to the data present in cloud. As encryption is provided at a same time decryption is also provided. The same key is used to decrypt which is used to encrypt the data.

Expert Analysis: This module is planned to confirm the user's roles. Specialist agreements are started by the data owners. Expert key values are delivered by the key organization server. Keys and attributes are given by the main authority.

User: This module is used to access the recode of the user. Private and certified access models are used in this system of secure sharing personal record. User received the recode in encrypted form to use decrypted form the uses the same key. User can update the information and along with it user has authority to send request to other also.

IV. PERFORMANCE STUDY

The cryptographic system has scalability and efficiency which is estimated by the following three parameters of cost.

- Storage Cost
- Communication cost
- Calculation Cost

A. Storage Cost

The existing methods only consider one field. But the proposed system consists of both public and personal field. This storage cost of proposed system is used in one public field and one personal field. This automatically minimizes the key size which in turn also minimizes the communication size. So all information requires less space to store.

B. Communication Costs

Since the public key size is less and also the message is very small in size and the number of elements in that key also reduces the communication cost.

C. Calculation Cost

The domain security level is selected with cryptography to obtain the secret key. The cryptography based is used to calculate the security level which is based on the results it approximately takes 0.45 mins.

V. CONCLUSION

A framework of secure sharing of personal records is proposed. Considering moderately responsible of cloud service, and realized that the private record model have whole control of their own privacy through encrypting their personal files. This framework addresses the unique tasks taken by multiple personal record owners and users, in this there is greatly reduce the complexity of key while enhance the privacy assurances compared with previous works. An AES algorithm is used to encrypt the personal data, so that record can access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations.

It is likely to achieve secure sharing of personal health records and other files in cloud servers. Person can have complete control of their own privacy through encoding their personal record and other files to allow access to selective users. The unique trial introduced by multiple personal recode owners and users such as security and key complexities are deeply reduced by using encryption algorithm that has a key size of 56-bits. As Attribute Based Encryption is used to encrypt the personal recode, so that person can allow access not only to personal users, but also various users from public domains with different professional roles. On-demand user revocation with security is also achieved.

REFERENCES

[1] M. Li, S. Yu,Y. Zheng, ,K. Ren, &W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", IEEE Transactions on Parallel and Distributed Systems, vol. 24(1), pp. 131-143, 2013

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters,"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[3] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[4] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safe- guarded," http://articles.latimes.com/2006/jun/26/health/ heprivacy26,2006.

[5] S. Jahid, P. Mittal, and N. Borisov, "Easier:Encryption-Based Access Control in Social Networks with Efficient Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar. 2011.

[6] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," Master's thesis, Worcester Polytechnic Inst., 2011.

[7] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure Attribute-Based Systems," J. Computer Security, vol. 18, no. 5, pp. 799-837, 2010.

[8] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", NISTSpecial Publication 800-145

[9] Jing-Jang Hwang, Hung-Kai Chuang,Yi-Chang Hsu, Chien-Hsing Wu, "A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service," Proceedings of the 2011 International Conference on Information Science and Application, April 2011.

[10] Qian Wang,Cong Wang,KuiRen, Wenjing Lou,Jin Li, "Enabling Public Au- ditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transactions On Parallel And Distributed Systems, VOL. 22, NO. 5, MAY 2011.

[11] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in CCSW '09, 2009, pp. 55–66.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications Magazine,Feb. 2010.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of userattributes," 2009.[Online]. Available: http://purl.org/utwente/65471

[14] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM'10, 2010.

[15] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[16] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.