ISSN 2348 – 8034
Impact Factor- 3.155

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURE SHARING OF PERSONAL RECORDS IN CLOUD USING ENCRYPTION

Miss. Shwetambari G.Pundkar[*1] and Dr. G. R. Bamnote[2]
[*1]Department of Computer Science and Engineering, Sant Gadge Baba Amravati University Amravati,Maharashtra,India
[2]HOD of Computer Science and Engineering, Sant Gadge Baba Amravati University Amravati,Maharashtra,India

ABSTRACT

Personal record is information, which is stored in cloud. In managing the record, cloud computing plays a vital role, since small organizations are not affordable to keep own servers to maintain the personal record for cost and security aims. In this system, the record can be share in secure manner. Here the symmetric key encryption is used to encrypt the record. The encrypted records are going to be store in cloud. The maintaining recodes in cloud are subjected to privacy and high risk of getting misused. There are various encryption methods to provide security and privacy in Cloud for records of user. Costly logical and results are open which shows the security, scalability and efficiency of our proposed scheme.

Keywords- *Cloud computing, Authentication, Security.*

I. INTRODUCTION

Personal record is a confidential data of the user, which is stored in cloud computing to gain cost benefit and better access control. In keeping Personal Record, cloud computing plays an important role, since small organizations are not reasonable to keep own servers to maintain the personal record for cost and security aims. Cloud computing is an advanced computing standard which has tired wide attention from both industrialists and scholars. Since cloud computing shares extent means through the internet in the open situation, thus security difficulties are important topics to address by emerging application programs which will protected to work top for medical use. By merging a set of current and new methods from research areas such as Service Oriented Architectures and Virtualization, cloud computing is seen as a computing pattern where data resources are stored over at the platonic world of Internet. Medicinal data is private and sensitive in nature. Cloud computing delivers clients a new way to share data assets and services that belong to various organizations. Privacy could only be used by the right persons, such as the particular doctor. A higher point of user's privacy is sure by exploiting multi expert symmetric key encryption. The arrangement also delivers run time change of access file attributes, supports capable on-demand user to access emergency scenarios. Widespread systematic and experimental results are obtainable which show the security, scalability, and efficiency of our planned scheme.

II. LITERATURE REVIEW

Up till now the effort was enforced to access data by attribute based encryption. Each and every data of user is in cloud but in encrypted form. Attribute based encryption technique is used to convert the plain text into cipher text. To progress the scalability of the encrypted data, one-to-many encryption methods such as ABE can be used. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. Personal record is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. To realize access control, the traditional public key encryption based schemes either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys.

Li et al.'s has introduced a Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. In this system the personal records should only be available to the authenticated users who are given the decryption key, while remain confidential to the other users. To confirm user's isolation control over their own recodes, it is important to have fine-grained data access regulator instruments that work with semi-trusted servers that is cloud. They have make available a analysis of the complexity and scalability of the recommended secure personal recode of sharing solution, in terms of many metrics in computation, communication, storage, and key management. They also link the scheme to several previous ones in complexity, scalability and security [2].Hur and Noh has introduces Fine grain access control which is the requirement of systems to usable. Till now systems can accomplish by applying access controls over the system because the facts and the claim most likely

ISSN 2348 – 8034
Impact Factor- 3.155

to be in the same trusted domain. On the other hand, the proposed systems and with the developing of data in the cloud, the data and the users are not on the same important domain [3]. Likewise, the data itself is stored in untrusted surroundings from which the data vendor wants it to be protected too. There are attribute based encryption technique systems which introduces a Cipher text-Policy Attribute-Base Encryption. On the other hand, this System wants some of fine grain access control; this introduces an improvement over the system to add an efficient user overturning. The keys related with the attributes must be changed and the les must be re-encrypted, also the new keys must be re-distributed [3] [5].

Hwang et al.'s has introduces the encryption system allows a presenter to send an encrypted message to a run time chosen subset of a given set of operators, such that only users in this subset can decrypt the message. An important element of programme encryption schemes is overturning of users by the broadcaster, thereby fill in the subset. Reversal may be either short-term, for a definite cipher-text, or enduring. The first public key broadcast encryption scheme with permanent revocation of users, unlike all previous public key schemes that support temporary revocation. The system explores the experiment of preserving user's privacy in automated health record systems [4].The architecture of cloud is containing of two parts Front End and Back End as shown in following figure:

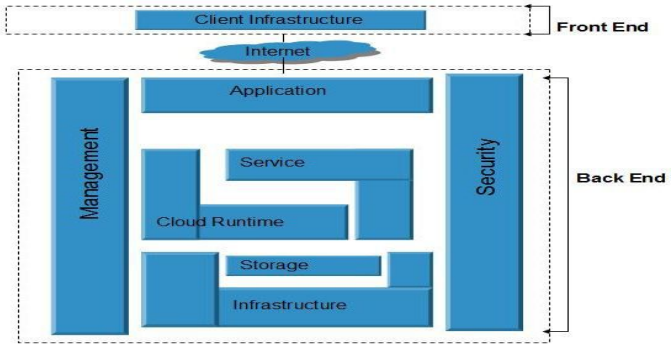

Figure 1.1: Cloud computing Architecture

- Front End:

Front End includes client infrastructure. It provides interfaces and applications that are necessary to access cloud computing platforms. Example is web browser.

- Back End:

Back End includes cloud components. Various applications provided by it, services, storage strategies, infrastructures are included by this. Some techniques that contribute to cloud computing:

- Application Programming Interface (API):

Without APIs it is hard to imagine the existence of cloud computing. The whole bunch of cloud services depend on APIs and allow deployment and configuration through them. Based on the API category used control, data and application, different functions of APIs are invoked and services are rendered to the users accordingly [19].These were the few technological advances that led to the emergence of Cloud computing and enabled a lot of service providers to provide the customers a hassle free world of virtualization fulfilling all their demands .

- Virtualization:

Virtualization is a technique, which allows sharing single physical instance of an application or resource among multiple organizations or tenants (customers). It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource when demanded .Creating a virtual machine over existing operating system and hardware is referred as Hardware Virtualization. Virtual Machines provide an environment that is logically separated from the underlying hardware. The machine on which the virtual machine is created is known as host machine and virtual machine is referred as a guest machine. This virtual machine is managed by a software or firmware, which is known as hypervisor [6].

Chase et al.'s has improved the Privacy and Security of Multi-Authority by Attribute-Based Encryption technique. They also propose a solution which removes the trusted central authority, and protects the users' privacy by preventing the authorities from pooling their information on particular users, thus making ABE more usable in practice. The solution in that work is to require that each user have a unique global identifier, which they must

ISSN 2348 – 8034
Impact Factor- 3.155

present to each authority. A user must present the same GID to each authority, it is very easy for colluding authorities to pool their data and build a "complete profile" of all of the attributes matching to each GID. However, this might be undesirable, particularly if the user uses the ABE system in many different settings, and wishes to keep information about some of those settings private [5].Lewko et al.'s has proposed a Multi-Authority Attribute-Based Encryption (ABE) system. In their system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can only act as an attribute based encryption authority by creating a public key and give out private keys to many users that recto their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, the system does not require any central authority. In constructing of the system, the largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority \tied" together different components (representing different attributes) of a user's private key by randomizing the key [16]. However, in this system each component will come from a potentially different authority, where they assume no coordination between such authorities. They created new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. They also proved that the system secure using the recent dual system encryption methodology where the security proof works by rest converting the challenge cipher text and private keys to a semi-functional form and then arguing security[6].

III. PROPOSED SYSTEM DESIGN

There are two main workings first are of user and second is of department. The user goes through the following step:

Authentication is checked; if the user has registered then the particular user can able to open this account otherwise user has to registered first. User has total four actions:

- Update detail
- View record
- Add friends and
- Most important is record sharing.

In update detail user can edit the details of him/herself. When user edit the details database also get change automatically. In view record the user has to select the department and based on the department the record is displayed. For example if user selected medical department the all the records related to medical is displayed. From that list the particular record is selected. In add friend if one user has to send record to another user then it is compulsory that they much be friends otherwise records will not send. So for that; user first send request to the desired used and that used will accept the friend request. Once they become friends the records can be easily send. In record sharing, the can be easily send from one user to another if they are friends. The records can be sent in encrypted manner. And at receiver side it is decrypted. The other working is of department; in this there are three departments medical, Insurance and last one is of Police. Each has same working. Each department has its own used id and password. By using that user id and password it is decided that the particular department is authenticated or not. If the department is authenticated then they can perform two task;

- Create Record
- Edit Record.

In create record the department first select the user, and then generate the record of that user. Once the record is generated the database is automatically updated. The second action is of editing the record; if there is a change in the recode then the record can be updated and database also get updated.

IV. IMPLEMENTATION DETAIL AND COMPARISON

The attempt is made to prepare a system in which the personal records are shared using symmetric key encryption technique. To develop this system implemented different modules. Proposed system modules are as follows:

ISSN 2348 – 8034
Impact Factor- 3.155

1. User Registration Module
2. Admin Module
3. Departmental Module
4. Record Sharing Module

By using these modules the execution of the project is completed.

- User Registration Module:

User registration is module in which the user is able to login the main application. User has to fill the entire registration field. After registration the user will login to application with their ID and password. Following are the authority provided to user by the admin: user can edit detail, view record, send record, receive record, send friend request, accept friend request, record visibility, account setting, change password, search friend, view friend, send message, receive message, forget password. All this facility is provided for user.

- Admin module:

Admin module plays a very important role in the secure sharing of personal record system. Only admin has an authority to create or to delete the user. Admin has all the authority of the project. All important action is performed by admin. User can register in using registration field but departmental registration is done by the admin. Admin will register only those departments which are authorized. And if admin comes to know that the particular department is using their power in illegal manner then admin has a right to delete the account of the department. Following are action perform by the admin: departmental registration, edit detail, change password, user and departmental account delete, emergency registration of department, account setting and Admin login.

- Departmental Module:

Departmental registration is under the admin. Admin will decide which department will register and which will not? There are three departments in this system: medical department, police department, LIC department. This entire department has their own work to perform. Following are action perform by the department: generate records of respective department; edit record, edit department, emergency registration, login, change password and account setting.

- Record sharing:

This most important module of the system is record sharing. By using this module the personal records of user can shared in secure manner. The sharing of records is done between user to user, users to department and department to department. The records are encrypted and then they are shared. The records are encrypted using symmetric key encryption. This technique is used for encrypting the record using the key and that same key is also used decryption. Key management technique is used for security purpose. The complete record is encrypted using AES encryption technique. Process of sharing record is as follow: Firstly the record is selected by user or department then the selected record is encrypted using AES algorithm and then the encrypted record is shared between user to user, users to department and department to department. This above process is done by sender side. At receiver side the received record is decrypted using the same key. The record will be decrypted only if the authenticated key is available. If the key is not available then the user will not able to decrypt the encrypted record and it the key is available the record can be easily encrypted.

V. COMPARATIVE RESULTS AND DISCUSSION

ISSN 2348 – 8034
Impact Factor- 3.155

For encryption and decryption of records, Advanced Encryption Standard (AES) algorithm is used. AES is the most secure symmetric encryption technique that has gained worldwide acceptance. It plays an important role in the security of data transmission. Cipher and Inverse Cipher are composed of specific number of rounds (Table 1). For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key length.

Type	Block Size Nbwords	Key Length Nkwords	Number of Rounds Nr
AES -128 bits key	4	4	10
AES -192 bits key	4	6	12
AES -256 bits key	4	8	14

Table 1: Comparison of block size, key length and number of rounds of AES keys.

Many encryption algorithms have been developed and implemented in order to provide more secured data transmission process and hiding sensitive information in cloud computing environment. Then main features of secure sharing of personal record system are security, Data management, Sharing, Record Keeping, Records type, Storage Capacity Search. Usually lightweight encryption algorithms are very attractive for applications. Through the research a fast lightweight encryption algorithm to secure the data from unauthorized access. For security of data, an encryption algorithm is based on AES using symmetric key encryption algorithm. The encryption and decryption time is one of the very important parameter while observing performance of any kind cipher. The below shows how much time the various AES standards will take in encrypting and decrypting the biggest size of data respectively. Theoretical analysis and experimental results of the achievement makes it very suitable for high rate and less overhead on the data. For all these compensation it is suitable for any large scale text and image transfer. The comparison of all algorithms is shown below:

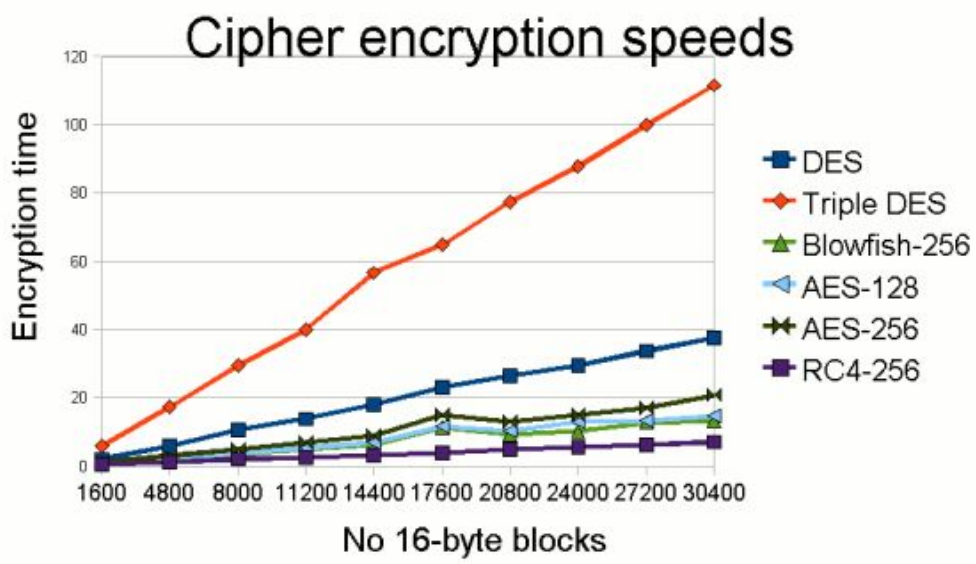

Figure 4-1: Comparison of all algorithms.

Each record in secure sharing system is encrypted and then it is sent for security purpose. In figure 4-2 the comparison is of plain and encryption is shown. The plain records required less time as compared to encrypted record but while during sending the record it is not encrypted means it has no security. But when the record is first encrypted and then it is sent it requires some time but it has more security. It has more security as compared to plain record.

ISSN 2348 – 8034
Impact Factor- 3.155

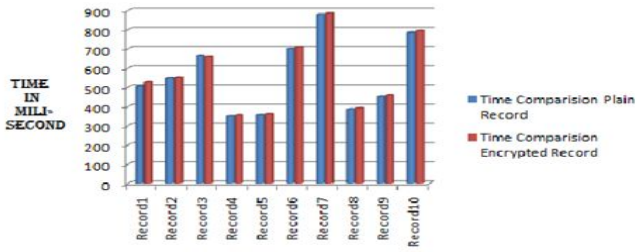

Figure 4-2: Comparison of plain and encrypted record

It is observed that use of AES algorithm transfers data file data file securely and in less time as compare to all algorithms. And also because of that an attempt is made to access each virtual cloud independently .So efficiency of data on cloud database is possible.

VI. CONCLUSION

In this paper the framework of sharing the personal record of the user is introduced. The used the symmetric key encryption is made to encrypt the data in the cloud. Whenever the data is in the cloud that data is in encrypted form and when the data has to retrieve from cloud it should be decrypted by using a key. So a novel framework of secure sharing of personal records in cloud computing is proposed. The different symmetric key algorithm have been considered for various file structures like diverse data type, data density, data size and key size, and analysed the variation of encryption time for different selected cipher algorithms. From the simulated results it is concluded that encryption time is does not dependent upon data type and date density of the file. The research revealed that; encryption only depends upon the number of bytes present in the file. It also revealed that encryption time and data size is proportional to each other. As the size of data increase the encryption time also increase proportional to data size and vice versa.

To enhance the data access control to the multiple departments work can be carried out. Currently the system is limited to only three departments. So there is a possibility of making this system larger by adding multiple departments. So when the system will be large enough then it can deploy globally. Further it can be integrated for e-health card systems or alternatives into privacy domains and address usability problems in this area.

REFERENCES

1. *S. G. Pundkar and Dr G.R. Bamnote, "Access of Encrypted Personal Record in Cloud", IJRITCC Vol: 3 Issue: 1 pp.326 – 329 January 2015*
2. *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*
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. *J.J Hwang, H. K. Chuang ,Y. Chang, C. Hsing, "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.*
5. *M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009*
6. *A. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," EUROCRYPT: Proc. 30th Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588, 2011.*
7. *J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, "Self-Protecting Electronic Medical Records Using Attribute-Based Encryption," Cryptology e-Print Archive, Report 2010/565, http://eprint.iacr.org/, 2010*
8. *M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.*

ISSN 2348 – 8034
Impact Factor- 3.155

9. *S.D.C Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data," Proc. 33rd Int'l Conf. Very Large Data Bases (VLDB '07), pp. 123-134, 2007.*
10. *S. Patil and K. N Reddy, "Overview of Efficient and secure Personal Health Record storing in cloud computing," IJISET Vol. 1 Issue 4, 275 - 279 June 2014*
11. *Prasad P S and Dr. G F Ali Ahammed, "Attribute Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing" www.ijcsit.com IJCSIT Vol. 5 (4) , 2014, 5038-5040//*
12. *A G Rudraxi, and P Nayak,"A Novel Patient Centric Framework for Data Access Control in Semi-trusted Cloud Servers", IJCSMC, Vol. 3, Issue.6, June 2014, pg.1 – 10*
13. *A. Sachdev and M.Bhansali, "Enhancing Cloud Computing Security using AES Algorithm", IJCA Volume 67– No.9, April 2013 pg.19-23*
14. *D.B.Lafky and T.A. Horan, "Prospective Personal Health Record Use Among Different User Groups: Results of a Multi-wave Study" at 41st Hawaii International Conference on System Sciences – 2008*