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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Concession on Allocation of Report in Cloud Using Aspect Based Cryptography

S.Raja shree[1], B. Sundar Raj*[2]

[1]Professor & Head, Dept. of CSE, Jerusalem College of Engineering, Chennai, Tamil Nadu, India

[2]Associate Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, India

*Corresponding Author

ABSTRACT: Data Security is an emerging need of information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal information could be exposed to those third party servers and to unauthorized parties. To assure the users control over access to their own records, it is a promising method to encrypt the records before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to records stored in semi-trusted servers. To achieve fine-grained and scalable data access control for records, we leverage attribute based encryption (ABE) techniques to encrypt each users record file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the record system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of user privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes.

KEYWORDS: cloud computing, security , encryption techniques , attribute based encryption

I. INTRODUCTION

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. Cloud computing services are seen as future of web world. There are several pros and cons associated with cloud computing. Here is brief descriptions of which type of user can enjoy the benefits of cloud computing which should avoid using cloud computing. Few of the disadvantages associated with cloud computing are

High Speed Internet - Cloud Computing performance in slow speed internet connections is absurd. Slow connections like dial-up make is Cloud computing a pain for the user or it can be say it is impossible for the users to enjoy cloud computing on slow connections. Large documents and web-base applications need a lot of bandwidth to download.

Constant Internet Connection – Cloud Computing without proper internet connection is just like lifeless body. Because you are using internet for accessing both your documents and applications, in case if you don’t have an internet connection you can’t even access your documents.

Limited Features – today many web-based applications are not fully featured when compared to their desktop versions. Just for an example there are n-number of things which can be done using Microsoft PowerPoint with the help of Google Presentation’s web based feature.

Unsecure Data – All the data in Cloud Computing is stored on Cloud. Concept of cloud computing is new and even

10.15680/ijircce.2015.0305208

II RELATED WORKS

H. L¨ohr, A.-R. Sadeghi, and M. Winandy, in 2011 "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, IEEE Project**.**In this paper, we endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve,and remain largely open up-to-date. To this end, we make the following main contributions and propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings.

M. Li, S. Yu, K. Ren, and W. Lou, 10, Sept. 2010, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm pp. 89–106.Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grainedaccess control to PHR data in a scalable .

M. Li, S. Yu, N. Cao, and W. Lou, 11, Jun. 2011. "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCSRecently, personal health record (PHR) has emerged as a patient-centric model of health information exchange, which features storing PHRs electronically in one centralized place, such as a third-party cloud service provider. Although this greatly facilitates the management and sharing of patients' personal health information (PHI), there have been serious privacy concerns about whether these service providers can be fully trusted in handling patients' sensitive PHI. To ensure patients' control over their own privacy, data encryption has been proposed as a promising solution. However, key functionalities of a PHR service such as keyword searches by multiple users become especially challenging with PHRs stored in encrypted form. Basically, users' queries should be performed in a privacy preserving way that hides both the keywords in the queries and documents.

.K. D. Mandl, P. Szolovits, and I. S. Kohane, Feb. 2001. "Public standards and patients' control: how to keep electronic medical records accessible but private,"

BMJ, vol. 322, no. 7281, p. 283.A patient's medical records are generally fragmented across multiple treatment sites, posing an obstacle to clinical care, research, and public health efforts. [1]Electronic medical records and the internet provide a technical infrastructure on which to build longitudinal medical records that can be integrated across sites of care. Choices about the structure and ownership of these records will have profound impact on the accessibility and privacy of patient information. Already, alarming trends are apparent as proprietary online medical record systems are developed and deployed.

J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, 09, 2009 "Patient controlledencryption: ensuring privacy of electronic medical records," in CCSW ', pp.103–114.

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when finegrained data access control is desired, and thus do not scale well. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

.S. Yu, C. Wang, K. Ren, and W. Lou, Oct , 2010 "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE INFOCOM'*.Current security mechanisms pose a risk for organizations that outsource their data management to untrusted servers. Encrypting and decrypting sensitive data at the client side is the normal approach in this situation but has high communication and computation overheads if only a subset of the data is required, for example, selecting records in a databatable[1][2].

In this paper, the sharing of records in a secure process are the main scope of the project. Thus the records are encrypted for secure transmission of datas. The public keys are transmitted to the users, addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes,. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial[3][4].

III. SYSTEM ANALYSIS

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers. There are many security and privacy risks which could impede its wide adoption. The main concern is about the patients could not have full control over her sensitive personal health information (PHI), especially when they are stored on a third-party server.Due to the high value of the sensitive personal health information (PHI), the third party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization. Letting each user obtain keys from every owner who's PHR she wants to read would limit the accessibility since patients are not always online[7][8]. The last contribution is the recommendation of credit application fraud detection as one of the many solutions to identity crime. Being at the first stage of the credit life cycle, credit application fraud. We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher[5][6].

TABLE 1: Various Testing

MODULE	TESTING PROCESS	RESULT	ERROR
Authentication Phases	The login page and Register page consists of username and password. The text boxes are	The authentication phase is successfully executed	An unsuccessful login occurs when wrong username or password is entered.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

	filled.		
Record Manipulation	The record manipulation phase consists of records which are encrypted by the users and stored in the database.	The manipulations of records are successfully executed.	Encryption error occurs when invalid file is uploaded.
Implementation of Multiple Authority	Various users are allowed to access the system by privilege based accessing of the system.	Request and obtain keys to the users, later provide keys to the specified owners.	Invalid key generation.

Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data.

IV. PERFORMANCE ANALYSIS

The maximum satisfactory response time to be experienced most of the time for each distinct type of user-computer interaction, along with a definition of most of the time. Response time is measured from the time that the user performs the action that says "Go" until the user receives enough feedback from the computer to continue the task. It is the user's subjective wait time. It is not from entry to a subroutine until the first write statement. If the user denies interest in response time and indicates that only the result is of interest, you can ask whether "ten times your current estimate of stand-alone execution time" would be acceptable. If the answer is "yes," you can proceed to discuss throughput. Otherwise, you can continue the discussion of response time with the user's full attention. The response time that is minimally acceptable the rest of the time[10][11]. A longer response time can cause users to think the system is down.

You also need to specify rest of the time; for example, the peak minute of a day, 1 percent of interactions. Response time degradations can be more costly or painful at a particular time of the day.

V. ARCHITECTURE

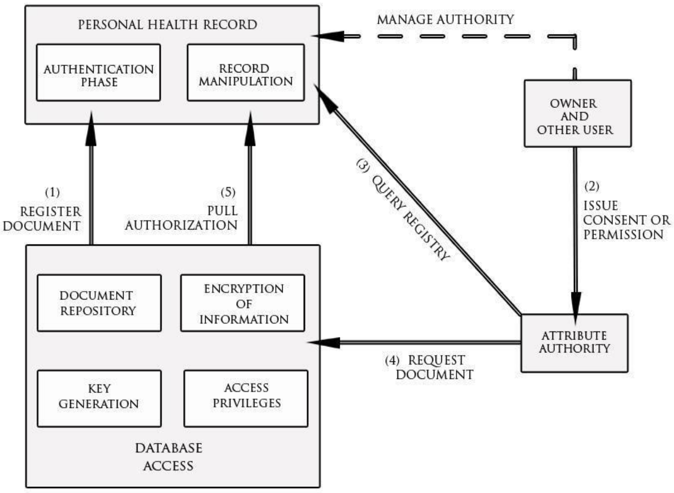

Fig 1.System Architecture

The profile development is the Central Authority of Scalable and Secure Sharing of Personal

Health Records. The Core Development is responsible for Register PHR owners and PHR users and theirs Login processes. It is also responsible for Profile maintenance of PHR owners and PHR users[12].

A. Multiple User Registration:

This module responsible for registering and removing accounts of PHR owners and PHR users in our framework.

B. Login:

This module responsible for enable login and logout processes for PHR owners and PHR users accordingly.

C. Database Maintenance

In this module the PHR owners, Personal users, Public users, Attribute Authorities can maintain their profile. All users can modify their profile such as edit, show or remove their profiles[13].

D. Record Manipulation

In this module the Record owner should decide how to encrypt her files and to allow which set of users to obtain access to each file. We refer to the two categories of users as personal and professional users, respectively. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users[14].

E. Access Control On Crisis :

The Owner shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. The Emergency Department(ED) responsible for provide break-glass key, for access PHER file due to the emergency. The emergency key set by the PHR owner while encrypting the PHR file[15][16].

F. Set Break-Glass Access:

When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department. To prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys.

G. Revoke Privileges:

After the emergency is over, the PHR owner can revoke the emergent access via the ED and the new break-glass key will be created. Thus the PHR is secure again and can be accessed by the users and PHR owner with a new set of keys. The setting up of acess of the encrypted PHR is enabled through three sets of functions implemented for ED attribute[17].

VI. CONCLUSION

Once the program exists, we must test it to see if it is free of bugs. High qualityproducts must meet user's needs and expectations. Further more the product shouldattain this with minimal or no defects, the focus being on improving products prior todelivery rather than correcting them after delivery. The ultimate goal of building highquality software is user's satisfaction.

REFERENCES

1. M. Li, S. Yu, K. Ren, and W. Lou, Sept. 2010, "Securing personal health records in cloud computing: multi-owner settings," in *SecureComm'10*, pp. 89–106.
2. Sathyanarayana H.P., Premkumar S., Manjula W.S., "Assessment of maximum voluntary bite force in adults with normal occlusion and different types of malocclusions", Journal of Contemporary Dental Practice, ISSN : 1526-3711, 13(4) (2012) pp.534-538.
3. H. L¨ohr, A.-R. Sadeghi, and M. Winandy, 10, 2010 "Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, ser. IHI , pp. 220–229.
4. Selva Kumar S., Ram Krishna Rao M., Deepak Kumar R., Panwar S., Prasad C.S., "Biocontrol by plant growth promoting rhizobacteria against black scurf and stem canker disease of potato caused by Rhizoctonia solani", Archives of Phytopathology and Plant Protection, ISSN : 0323-5408, 46(4) (2013) pp.487-502
5. M. Li, S. Yu, N. Cao, Jun. 2011, Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in *ICDCS*.
6. Subha Palaneeswari M., Abraham Sam Rajan P.M., Silambanan S., Jothimalar, "Blood lead in end-stage renal disease (ESRD) patients who were on maintainence haemodialysis", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(10) (2012) pp.1633-1635
7. K. D. Mandl, P. Szolovits, and I. S. Kohane, Feb. 2001, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, p. 283.
8. Sukumaran V.G., Bharadwaj N., "Ceramics in dental applications", Trends in Biomaterials and Artificial Organs, ISSN : 0971-1198, 20(1) (2006) pp.7-11.
9. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter *09*, 2009, "Patient controlled encryption: ensuring privacy of electronic medical records," in *CCSW*, pp. 103–114.
10.Selva Kumar S., Ram Krishna Rao M., Balasubramanian M.P., "Chemopreventive effects of Indigofera aspalathoides on 20-methylcholanthrene induced fibrosarcoma in rats", International Journal of Cancer Research, ISSN : ISSN: 1811-9727, 7(2) (2011) pp.144-151.
11.S. Yu, C. Wang, K. Ren, and W. Lou *'10*, 2010, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *IEEE FOCOM*.
12. C. Dong, G. Russello, and N. Dulay , 2010, "Shared and searchable encrypted data for untrusted servers," in *Journal of Computer Security*.
13. V. Goyal, O. Pandey, A. Sahai, and B. Waters *'06*, 2006, "Attribute-based encryption for fine-grained access control of encrypted data," in *CCS*, pp. 89–98
14.M. Li, W. Lou, and K. Ren , Feb. 2010, "Data security and privacy in wireless body area networks," *IEEEWireless Communications Magazine*.
15.A. Boldyreva, V. Goyal, and V. Kumar, 08, 2008, "Identity-based encryption with efficient revocation," in *ACM CCS*, ser. CCS pp. 417–426.
16.L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, 2009 "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes,".
17. S. Yu, C. Wang, K. Ren, and W. Lou, *10*, 2010, "Attribute based data sharing with attribute revocation," in *ASIACCS*.
18. Dr.K.P.Kaliyamurthie, D.Parameswari, Load Balancing in Structured Peer to Peer Systems, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 22-26, Volume1 Issue 1 Number2-Aug 2011

19. Dr.R.Udayakumar, Addressing the Contract Issue,Standardisation for QOS, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 536-541, Vol. 1, Issue 3, May 2013
20. Dr.R.Udayakumar, Computational Modeling of the StrengthEvolution During Processing And Service Of9-12% Cr Steels, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 3295-3302, Vol. 2, Issue 3, March 2014
21. P.Gayathri, Assorted Periodic Patterns Intime Series Database Usingmining, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 5046- 5051, Vol. 2, Issue 7, July 2014.
22. Gayathri, Massive Querying For Optimizing Cost – CachingService in Cloud Data, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 2041-2048, Vol. 1, Issue 9, November 2013