2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN)

Secured Health Care Information Exchange on Cloud Using Attribute Based Encryption

[1]Samydurai A,
[1]Department of Computer Science and Engineering
[1]Valliammai Engineering College,
[1]SRM Nagar, Kattankulathur, Chennai, India.
[1]asamydurai@gmail.com
[5]Cognizant Technology Solutions India Pvt. Ltd,
MEPZ, Chennai, India

[2]Revathi K, [3]Prema P, [4]Arulmozhiarasi D S, [5]Jency J,
[6]Hemapriya S
[2, 3, 4, 6]Department of Computer Science and Engineering
[2, 3, 4, 6]Dr VPR Nagar, Manimangalam, Chennai, India
[2, 3, 4, 6]Dhanalakshmi College of Engineering
[2]neyadharshini@gmail.com, [3]premapersonal@gmail.com,
[4]aun88.selvaraj@gmail.com, [5]jency.manoharan@gmail.com,
[6]hema.vs22@gmail.com

Abstract— **Personal health record (PHR) 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. This leads to address the privacy issues i.e., hide the sensitive health information of a patient, as the information can be accessible to unauthorized parties because of the nature of the storage. This paper describes novel patient-centric secure data sharing framework for cloud-based PHR systems. The paper is to create Health Care Information (HCIs) that are efficient and secure. HCIs can be stored in a third party cloud. The patients, who have created their profiles in the system, make their own HCIs, mentioning their disease, symptoms and other sufficient details. The doctors who are also a part of the system attend to the queries of the patients that have been updated in the cloud. The doctors' prescription is updated by the admin of the system, whereas the cloud admin has no access to the data. The level of encryption is considered before generating the encryption key. The record is then accessed using the key that the admin has generated. The health care services can look up to the user details. The details of the secured information remains encrypted, whereas the other details remain as updated.**

***Index Terms*—Health Care System, HCI, ABE, Cloud Computing**

I. INTRODUCTION

Health Care Information (HCIs) is a health information exchange that is related and managed by the patients, themselves. HCIs is often outsourced to be stored at a third party like cloud providers. This involves privacy issues since the sensitive health information can become accessible to the cloud providers and at times, to unauthorized parties. This makes encryption mandate. The data should be encrypted by a trusted method that performs encryption before the data is outsourced and stored in the cloud. Encrypting data would raise issues such as risks like sensitive data being exposed, a large number of keys to be generated, differences in security level provided by the system and expected by the user and inability to access during emergency. In this paper, we proposed a novel method to encrypt the data at different security levels, as the patient desires. Efficiency is achieved by dividing the users into two different domains. The domain containing doctors whom the patients send their queries to, can access the patient details. Whereas, the health care departments like insurance providers can access only the details that are insecure. Key revocation is used invalidate the existing key and generate a new one. This can be of great help in emergency scenarios when there is a demand for a new key.

II. RELATED WORK

Cloud computing became highly accepted and advantageous over the years since it serves the consumers with the computer infrastructure. This has made the computing paradigm has become the key in various industries. However, this boon of technology comes along with a list of issues to be addressed, the most important of which is security. Sensitive information can draw many intruders to extract information from the cloud. Cryptographic methods are used to maintain the security of data. This in turn produces a heavy computation overhead. We can achieve high security by using the combination of Attribute based Encryption (ABE), Proxy Re-encryption and Lazy Re-Encryption [8].

Health Care Systems require high cost of storing and maintaining health records. Hence managing the data about health information is highly essential. The system should be able to provide information to reliable consumers, when necessary. Hence, a system should be built, that is able to collect, maintain and manage all the records related to health information [1]. Mobile devices have been used to access patient information over the years. However, there is no standard for security. Hence, mobile devices were used after specific authentication [2].

The use of cloud computing technology in managing health records has given opportunities to the users and other personnel like heath care providers and insurance providers to manage health care information. However, the security of the information is questioned. The issues associated with the cloud-stored information have been analyzed and solutions have been identified. Architecture that provides a consumer controlled approach has been proposed to improve security

978-1-4673-6823-0/15/$31.00 ©2015 IEEE

[13, 14, 16]. Authentication and Encryption have been stated as the two steps that can effect in highly secured data. However, the encrypted data may require decryption during emergency. Hence, it is equally essential to invalidate the key and create a new one, when necessary [4]. Storing and exchanging of data was recorded and it required constant monitoring. It is called Continuity Care Document (CCD). Access control and security were made into effect using digital signature and encryption [5].

In order to reduce the cost of infrastructure and enhance the dynamic resource adjustment, a new mechanism called Bilinear Pairing was used [6]. However, the mechanism has limitations due to the number of challenges that the system had to face. Encryption based on attributes became to new paradigm in the recent years which can be used to ensure security. The attribute information is extracted to make the key that is used for encryption and decryption [3]. Information of the patient may be required by authorized third party. Patients would themselves like to reveal information. Hence, a system that analyzes the third party and provides access was developed [7]. To invalidate the key and generate a new one, revocation scheme was employed in various proposals. A scheme was proposed in which one attribute of the user was revoked instead of all the attributes [9]. Patient aware records were created that used strong authentication. Embedded mechanisms to provide access during emergency were also a part of the system [10].

An access control framework to deal with multi-authority systems was proposed with an efficient encryption scheme. This made multi-authority scheme scalable and efficient [12]. The problems to be addressed in data sharing [18, 19] led to many proposals, each describing various ways to solve security issues. Most of them proposed to provide keys to effect security access. However, it led to another challenge of the key escrow problem. Authorities had to deal with a wide pool of users to provide their keys. Proposals to build a system without the key escrow problem were made [11].Identity based broadcast encryption was employed in sensor networks to reduce key size. This caused computation and storage overhead. Systems were proposed in later years, which reduced both computational times and storage overhead [15]. However, attribute based encryption is the suitable method of encrypting the health records. The attributes that require high security can only be encrypted and the key to decrypt the file is created by using the values of attributes.

The paper is organized as follows: In Section III, we presented the framework of Health Care Information (HCI) Sharing system. Section IV gives a deep insight into the effective maintenance of HCI records in cloud with the help of attributed based key generation and encryption algorithm. Section V discusses the experimental analysis of secured HCI sharing in cloud. In section VI, we provided the conclusion of our work.

III. Framework for Health Care Information (HCI) Sharing

The profile of the patient is stored in the cloud database. The patient then updates his/her issues and queries as in the figure1. The patient is endowed with the ability to specify the doctor whom the patient wants to consult. This is again stored in the cloud database.

The doctor, when logging into his account views the queries of his/her patients. The cloud database in the system is accessed only by the registered patients and HCI Admin using Attribute Based Encryption. The doctor and healthcare departments can access the permitted data. The Cloud Admin does not have any access to the database, and thus ensuring efficiency and security over the data shared in the cloud.

The framework used Attribute Based Encryption (ABE) to avail security to the system. Attribute-based encryption (ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

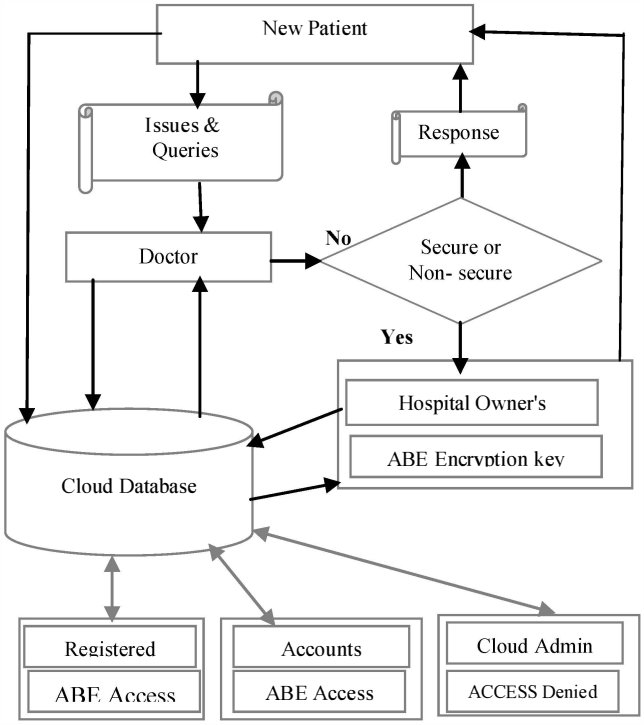

Fig.1 A Framework for Health Care Information (HCI) Sharing

IV. Storage of Health Care Information (HCI) in Cloud

Personal health record has emerged as a patient-centric model of health information exchange. A HCI service allows a patient to create, manage, and control their personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of their medical records and can share their health data with a

978-1-4673-6823-0/15/$31.00 ©2015 IEEE

wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many HCI services are outsourced to or provided by third-party service providers. The main concern is about whether the patients could actually control the sharing of their sensitive Personal Health Information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the other hand, 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 and security numbers and health problems was stolen by an employee who took the data home without authorization.

A. Limitation of Third Party Storage

Patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. Because a third-party server inside hackers can able to leak the patients' information and security records to other peoples so this scheme is not fully trust.

In Existing attribute-based encryption 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.

B. Enhancing the Security

We proposed a novel ABE-based framework for patient-centric secure sharing of HCIs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains. The doctors and health care constitute one domain. These are the users to whom the patients have addressed to. These users will be able to view the patient queries and reply to them. Other users like insurance personnel and pharmacists can view the details that are insecure. The encrypted information remains undecipherable to all the intruders. An added advantage is the specification of the level of encryption. This ranges from 0-4. Each level of encryption has a different type of key generated.

The system uses attribute based encryption (ABE) algorithm and the advantages of it are listed below.

Advantages:

- Our proposed secure HCI sharing solution overcomes the issue of insecure access by third parties.
- Enhanced level of security for the patient health information. After encryption and updating of the personal health information by the admin, the patient gets a key to decrypt the information.
- The key generated is based on the values of the attributes provided by the user during registration.
- The key generation is dependent on the security level, ranging from various levels that are insecure to highly secure
- Undesirable access of data by users like pharmacists, insurance personnel are restricted.
- Patients have full privacy control over their HCIs.

C. Secured HCI Sharing System

The main objective of the framework is to provide secure and efficient HCI access and efficient key management at the same time. The Health Care Information consists of various patient details including basic information like name, age, user id, contact information like phone number, address and health details like blood group. The various users of the system are the patients, doctors and health care providers and the agent who requires information. The owner of a HCI is the patient who created it. The patient can address his queries to the doctor of his choice.

There could be a number of users who wish to access this HCI. The key idea is to divide the users who access the patients' HCI into two different domains. The domain consisting of doctors can view all the HCI records that have been addressed to them. This domain consists of doctors and other health care providers. The patients must create their profiles to access the system. The details of the doctors must be uploaded so that they are given access to the records of the patients who contact them. The doctors answer queries by logging into the system and viewing the records to which they reply. It is expected of the doctor to send back the prescription that the patient must follow and comments to share additional information and directions to the patients.

In this framework, the generation of the key is based on the attribute values given by the user. For example, it could be from the basic details provided in the profile. The user can have their data encrypted, based on desired security levels. Each level of security has a different way of generating key.

Security levels range from 0 to 4, which can be chosen during encryption. Choosing the LEVEL-0 would generate a key with no character. LEVEL-1 of security causes key generation only with numbers. LEVEL-2 of security when chosen creates key consisting of small characters and numbers only. A combination of small characters, large ones and numbers is used for key generation in the security level named LEVEL-3. Special characters, small and large characters along with numbers are used to generate key in the level of high security, LEVEL-4.

The Table 1 given below presents a comparative measure of various attribute based encryption algorithms. It is clearly visible from the Table 1, the MA-ABE provides better access control. Comparatively to other, MA-ABE leads to average computational overhead and it is efficient.

TABLE 1 Comparison of Attribute Based Encryption Algorithms

Models	ABE	KP-ABE	CP-ABE	HABE	MA-ABE
Fine gained Access control	Poor	Poor and Good if there is reencryption technique	Average	Good	Excellent
Efficacy	Average	Average	Average	Elastic	Scalable
Collision resident	Average	Excellent	Excellent	Excellent	Elevated

978-1-4673-6823-0/15/$31.00 ©2015 IEEE

A Multi-Authority Ciphertext-Policy Attribute-Based Encryption (MA-CP ABE) system[17] which is a variation of Multi Authority Attribute Based Algorithm (MA-ABE) is comprised of the following five basic operations listed as below:

1. Global Setup(Φ) → GP

This is the first operation and it takes Φ as the security parameter and outputs GP as Global Parameter

2. Authority Setup(GP) → SK, PK

This takes GP as input parameter and outputs the Secret Key and Public Key pair, respectively as SK and PK.

3. Encrypt(M,(A, λ),GP,{PK})→CT

The message M is encrypted through an access matrix (A, λ), the set of public keys of relevant authorities with the global parameter GP. It produces the Cipher-Text CT as output using the equation1 given below.

$$CT = M\left(\prod_{A \in SK} PK_A^{''}\right) \quad (1)$$

4. KeyGen (GID, GP, i, SK) →K_i, GID

KeyGen takes an identity GID from the global parameter GP, an attribute i which belongs to some authority, and the secret key SK. It Outputs an identity pair as the respective key of an attribute as K_i and GID for that.

5. Decrypt (CT,GP,{K_i,GID}) → M

The decryption is done with the help of key and identity pair generated in KeyGen operation over the global parameter GP. It outputs either the message M when the collection of attributes i satisfy the access matrix corresponding to the cipher-text and it uses the following equation 2 for decryption. Otherwise, decryption fails.

$$M = CT(\prod_{i \in SK} SK_{i,GID}) \quad (2)$$

With the help of algorithm stated above the data updated by the patient and the prescription made by the doctor is encrypted after the key is generated. The admin can select the specific attributes that require encryption. This could include sensitive information like disease and symptoms uploaded by the patient, prescription and comments made by the doctor. If the patient demands a highly secure profile, all the attributes can be selected and encrypted.

Under the assumption, that the cloud server is not a trusted party. The information stored in the cloud can be accessed by the cloud admin. Health information specifically draws a lot of attention since it may be required by a number of parties. Health Care details may be required by pharmacists who might make a note of diseases and prescriptions to acquire a note of medicine in demand, patients who require medications and other details related to his business. The insurance department may require information to know the health condition of patients to deal with insurance policies. Such high demand may cause the cloud admin to fetch the information stored by the patients and doctors. Due to lack of credibility, the cloud admin is given no powers to fetch the data. However, the cloud admin can view the encrypted details. The admin of the system alone has the authority to encrypt the details. All other users who want to acquire details can access only the encrypted details.

V. PERFORMANCE

The Figure 2 gives the snapshot of home page of our proposed system which allows secured data i.e. HCR of patients.

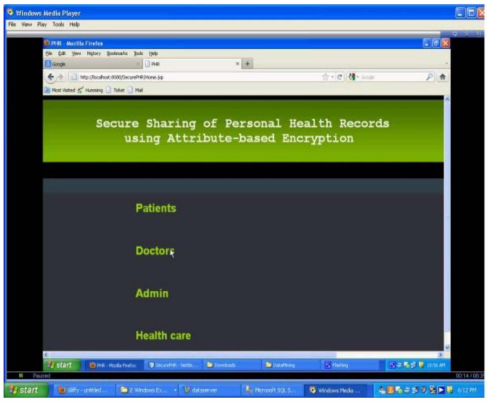

Fig. 2. Home Page of Proposed System

The Figure 3 describes the comparison of all the security levels available in the proposed system. The vertical axis quantifies the level of security. The horizontal axis holds percentage of obtained security as a quantitative measure. The raise of the line in the graph describes the characters that each key to be generated is made up of. The 0th level of security includes no character in the key. This is the lowest security range and is quantified to have '1' as the security level. This can be termed as 'Insecure'. Patients who do not prefer secure profiles and don't mind to offer a view of their profiles to the insurance agents and pharmacists can use this type of security in their records.

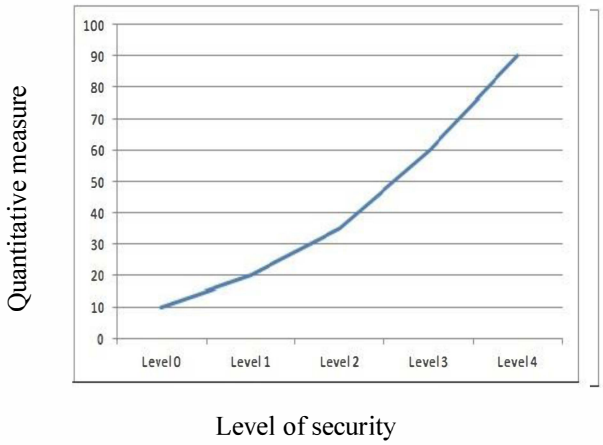

Fig. 3. Comparison of Levels of Security Proposed

978-1-4673-6823-0/15/$31.00 ©2015 IEEE

VI. CONCLUSION

In this paper, we presented a HCI sharing system that can be used to store sensitive health information which can be outsourced in the cloud with high security. The patients can send queries to specified doctors which are updated in the cloud. The doctors can reply to the queries which is updated and then encrypted by the admin. The patients view the details after proving the encryption key. The details remain encrypted to other users who view the health care information, ensuring the increased security.

REFERENCES

[1] Atsuo, Chujyou, Hiroshi, Kato, Shinobu, Yoshitaka, "Analysis and Design of Personal Health Record Management System", International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), pp.800 – 805, 2013, doi:10.1109/SITIS.2013.1302013.

[2] Bryhni. H, Mirkovic. J, Ruland C.M, "Secure solution for mobile access to patient's health care record", e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on, pp. 296 – 303, 2011, doi: 10.1109/HEALTH.2011.6026769.

[3] Changji Wang, Yang Liu "A Secure and Efficient Key-Policy Attribute Based Key Encryption Scheme', International Conference on Information Science and Engineering, 2009.

[4] Cheng Hong, Dengguo Feng. Min Zhang, Zhiquan Lv, "A secure and efficient revocation scheme for fine-grained access control in cloud storage", IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), 2012, pp. 545 – 550, 2012,doi: 10.1109/CloudCom.2012.6427602.

[5] Chen.R.J, Hsieh.G, "Design for a secure interoperable cloud-based Personal Health Record service", IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), pp. 472 – 479, 2012, doi: 10.1109/CloudCom.2012.6427582.

[6] Chia-Hui Liu, Fong-Qi Lin, Dai-Lun Chiang, Tzer-Long Chen, Chin-Sheng Chen, Han-Yu Lin, Yu-Fang Chung, Tzer-Shyong Chen, "Secure PHR Access Control Scheme for Healthcare Application Clouds". ICPP 2013: 1067-1076

[7] Gorp, P.V., Comuzzi, M., Fialho, A.S. and Kaymak, U, "Addressing health information privacy with a novel cloud-based PHR system architecture", 2012, doi:10.1109/ICSMC.2012.6378006

[8] Cong Wang, Kui Ren, Shucheng Yu, Wenjing Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing", Proceedings of the 29th conference on Information communications pp. 534-542, 2010, ISBN: 978-1-4244-5836-3.

[9] Dengguo Feng, Liwu Zhang, Qiang Li ,"An attribute based ncryption scheme with fine-grained attribute revocation", Global Communications Conference (GLOBECOM), pp. 885 – 890,2012, doi: 10.1109/GLOCOM.2012.6503225.

[10] Huda. M.N, Sonehara.N, Yamada.S, "Privacy-aware access to Patient-controlled Health Care Information in emergency situations", 3rd International Conference on Pervasive Computing Technologies for Healthcare, PervasiveHealth 2009,pp. 1– 6,doi: 10.4108/ ICST. PER VASIVEHEALTH 2009.6008

[11] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing", *IEEE Trans. on_ Knowledge and Data Engineering*, pp. 2271 – 2282, Vol.:25 , No. 10,2013, 10.1109/TKDE.2011.78.

[12] Kan Yang, Xiaohua Jia, "Attributed-Based Access Control for Multi-authority Systems in Cloud Storage", IEEE 32nd International Conference on, Distributed Computing Systems (ICDCS), 2012 pp. 536 – 545, doi: 10.1109/ICDCS.2012.42.

[13] Li J, "Privacy policies for health social networking sites" *J Am Med Inform Assoc*. 2013;20(4):704-7.

[14] Ling Liu, Rui Zhang, "Security Models and Requirements for Healthcare Application Clouds", Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing pp. 268-275,2010, ISBN: 978-0-7695-4130-3.

[15] Shuaishuai Zhu, Xiaoyuan Yang, Xuguang Wu, "Secure Cloud File System with Attribute Based Encryption", 5th International Conference on Intelligent Networking and Collaborative Systems (INCoS), pp. 99 – 102,2013, doi: 10.1109/INCoS.2013.22.

[16] C. Sunil Kumar, A. Samy Durai, S.R. Vinotha, "Privacy and security solutions for interoperable health information exchange", Int. J. of Medical Engineering and Informatics, 2013 Vol.5, No.2, pp.137 - 144.

[17] Yannis Rouselakis, Brent Waters, "Efficient Statically - Secure Large Universe Multi - Authority Attribute-Based Encryption", IACR Cryptology ePrint Archive 2015: 16 (2015).

[18] Samydurai, A & Shanmugam, A 2014, 'Data Sharing in a File Structured QoS Aware Peer-to-Peer System', Research Journal of Applied Sciences, Engineering and Technology, Vol 7(19), ISSN: 2040-7459, pp.3995-4001.

[19] Samydurai, A & Shanmugam, A 2014, 'Efficient Tree based Caching for Efficient QoS Peer-to-Peer File Sharing', Proceedings of the International Conference on Information Technology and Management, WIT Transactions on Information and Communication Technologies, WIT Press , Vol.49, pp.707-714, ISSN: 1743-3517.

978-1-4673-6823-0/15/$31.00 ©2015 IEEE