Privacy Preserving Data Storage And Auditabillity In Mobile-Access Of Health Data On Clouds

Mr. Saquib Ahmed
Department Of Computer Science & Engg
Nagpur Institute of Technology
Nagpur, India
Email: saquib.ahmed2507@gmail.com

Prof. jagdish pimple
Department Of Computer Science & Engg
Nagpur Institute of Technology
Nagpur, India
Email:pimplejagdish@gmail.com

Abstract— In digital world today, communication and information technology are becoming an integral part in healthcare. Instead of keeping patient's health record in paper form inside a written file, you can find all patient related information stored in an organized and systematic database as well defined files using a specific system in almost every clinic. But those paper based files sometimes got lost or information was spread up in files in different hospitals so no one could see the whole scenario. From this point we come up with our idea to build security aspects of privacy and auditability into mobile healthcare with the help of private cloud. The system will offer privacy preserving data storage and retrieval along with efficient key management techniques for misusing the health record.

Keywords*-Auditability,privacy, key management, healthcare,cloud*

*****

I. INTRODUCTION

In the past, information about patients, the sickness they have had, when they had treatment and what medications were prescribed to them by a doctor was written down and kept in files inside hospitals where they have been treated. The drawback of trivial file system was that files got lost in several hospitals and doctors cannot get a clear picture about patient's history. The agenda is to make sure that doctors and other health professionals have the complete information about patient's health record which is important to help them to make the best decisions about the patient, their diseases and their treatment.

The electronic health care systems are dominantly increasing day by day as large amount of personal data for medical purpose are involved and once the health record is exposed to cyberspace it becomes vulnerable to the outside world. According to survey of government website [1], around 9 millions patient's health record was leaked in past three years. Despite the highest importance, privacy issues are not addressed efficiently at the technical level and efforts to keep health record secure have often fallen short. Automated decision support algorithms in mobile health monitoring [2] which is cloud based was considered future trend.

Unfortunately, the cloud assisted mobile-access of health data is promising and offers a great advance in healthcare systems and improves quality of life thus reducing the healthcare costs, there is dominant opposing force in making a technology reality. Without properly addressing the health record maintenance and data management the complete health record is subject to get breached during data collection.

This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of reliable protocols and architectures, which will assure the privacy and security to stand as a guard against the adversaries and possible threats.

II. LITERATURE SURVEY

As far as emergency medical services are concerned, one of the earliest works on e-healthcare is medical information privacy assurance (MIPA) [3].It was one of the few works that pointed out the important challenges for privacy of medical information. It has also put on lights on devastating privacy breaches that were caused by inefficient technology. MIPA developed privacy-protecting infrastructures and technology to facilitate the personalized development of health information.
Winandy and colleagues [4] have pointed out various drawbacks of current e-health solutions and standards. In particular they have not proposed the client platform security, which is sensitive aspect of security in e-health systems. Liang [5] and colleagues proposed efficient and patient-centric access control scheme which allows data requesters to have different access privileges which is called as role-based access, and then assigns different attribute sets to them. Performance analyses and extensive security mechanisms and demonstrate that the scheme is able to achieve desired security requirements with little amount of communication delay.

The cryptographic key-management solution for e-healthcare systems was proposed by lee and lee [6] and in their solution, the trusted server has the ability to access the health record at any time which could result a possible threat. Zhang and colleagues [8] proposed framework for privacy-preserving attribute-based authentication system in e-health networks.

The attribute-based authentication schemes designed for higher privacy levels preserve the more privacy on attributes and attribute values, but cost more computation and communication resources.

Terry and Gunter [9] designed a system so that it accurately captures the state of the patient at all times and represent data in suitable form. The system also had ability to view entire patient's history without the need to keep track of patient's previous medical record volume. It also assists in ensuring data is accurate, appropriate and legal. It has significantly reduced the chances of data replication as there is only one modifiable file, which means that the file is updated constantly when viewed at a later date or day and removed the issue of lost forms or paperwork.

Ren and colleagues [10] proposed e-health care system to which allows patients to encrypt their personal health records (PHR) before storing it on central authority. Because of the fact that the encrypted PHR prohibits the centralized server from obtaining the information it still faces the problem of data verification. Another drawback of this scheme is that it is vulnerable to single point of failure.

The concept of patient controlled encryption (PCE) was proposed by Horvitz [11] in which the health records are divided into hierarchy of smaller piece of information which will be encrypted using the key which is under patient's control. They provided a symmetric-key PCE for fixed hierarchy, a public-key PCE for fixed hierarchy, and a symmetric-key PCE for flexible hierarchy from RSA.

III. ELECTRONIC HEALTH RECORD

An electronic health record (EHR) is a digital version of a patient's paper based record. EHRs are nothing but the systematic and well organized patient's health record database which is real-time and patient-centered in nature that make information available instantly and securely to authorized users. Theoretically EHR is record in digital format which can be considered as capable of being shared across different health care systems. An electronic health record (EHR) is defined as a systematic collection of electronic health information about individual patients. EHRs may consist of a range of health related data, including medical history, demographics, medication and allergies, laboratory test results, radiology images, immunization status, personal statistics like age and weight, vital signs, and billing information. Health record in digital form and information systems are expected to improve quality of life and efficiency which will eventually lead to cost effective health care systems. The EHR typically includes:

- Basic contact information.
- Life insurance information.
- Medications.
- Allergies.
- Blood group and other health related data.
- Reference person in case of emergencies.
- Family Background.

IV. PROBLEM STATEMENT

Motivated by the security issues in electronic healthcare system which is assisted by the services of public and private clouds. We propose to employ privacy in mobile healthcare system. The system will offer security mechanism for storage of patient's e-health record, security will be privacy preserving data storage which will use various cryptographic techniques like symmetric search encryption for authentication of user for role-based access. Attribute-based encryption (ABE) is also used with threshold signing for user authentication.

Apart from privacy we propose to build auditability of authorized users to prevent misbehavior with same encryption techniques by combining ABE with threshold signing.

In order to enhance the security aspects, the system also employs efficient key management for privacy preserving data storage and it will use the pseudo random number generator for unlinkability. The elliptic curve Diffie-Hellman (ECDH) which combines elliptic curve and Diffie-Hellman key management techniques can be considered as future work for efficient key management mechanism.

V. PROPOSED WORK

Cloud computing technology has evolved with great deal today, and everyone is curious to know what exactly the technology is, while there is a general idea behind cloud that applications or other business functions exist somewhere away from the business itself. There is much iteration that companies are looking for in order to actually use the technology. Cloud computing is a promising platform which has offered variety of ways for businesses to increase their IT functionality without having to add infrastructure, personnel, and software in their business. According to the different types of services offered, cloud computing can be considered to consist of three layers [12]:

A. System models

- Product-as-a-Service (PaaS): In this type of service model, the user applications can be developed using the tools provided by the PaaS provider

- Cloud Software-as-a-Service (SaaS): In this model, the applications running on cloud provider's platform can be used by the user. The services provided by cloud provider can be accessed from any heterogeneous system or any interface. The privileges to use these services are limited with some defined usage.

- Cloud Infrastructure-as-a-Service (IaaS): This model has the ability to provide full specification usage to the user. It provides services like networks, storage, provision processing and other fundamental computing resources. This way enables the consumer to deploy and run arbitrary software, which can include operating systems and applications.

B. Threat Model

The private cloud is fully trusted by the user to carry out health data-related computations. Public cloud is assumed to be honest-but-curious, in that they will not delete or modify users' health data, but will attempt to compromise their privacy. Public cloud is not authorized to access any of the health data. The doctors are granted access rights to the health record only pertinent to the treatment, and only when emergency takes place.

In this paper we introduce the private cloud which provides the services to mobile users. As mentioned above, cloud software as a service (SaaS) provider provides services to the private cloud by using the infrastructure of public cloud providers like Google, Amazon etc. Every user outsources health related data to the private cloud which in turn stores the data and processes it on the public cloud. The system will offer privacy-preserving mechanisms since intensive and sensitive data is shifted to the cloud and huge amount of computations are involved.

We propose to design a efficient key management mechanism which will felicitate the implementation of privacy of the data stored on the private cloud provided by cloud service providers as SaaS. The system also focuses on an optimized retrieval scheme for the all the situations and especially for emergency situations where the retrieval of stored data stored on the cloud needs to be speed up. The system will also provide auditability which ensures the integrity of sensitive health care data present at cloud.

VI. METHODOLOGY

The cloud-based electronic health record and its model consist of three components: Searchable encryption, efficient key management and auditable access control. When doctors receive data from users, private cloud processes it and stores it on public cloud such that storage privacy and efficient retrieval can be carried out. Next Privates cloud involves in auditability scheme with users.

A. Storage privacy using searchable symmetric encryption (SSE)

The first component is storage privacy for electronic health record. System's storage mechanism is based on secure index or SSE. In this encryption technique, user can encrypt their data with additional data structures to allow for efficient search. As far as our model is concerned, the private cloud takes the role of a user, and public cloud is the storage server in SSE.

Zhang and colleagues [13], have shown the feasibility of secure index for health data storage privacy. They followed approach based on linked list data structure. There were several practical issues which have tried to put up in this paper.

1) The requirment related to unlikability was not well addressed and dealt here.The above work did not show how to make file indentifiers.It will be easy for attacker to panetrate multiple files from same user.

2) Traditional SSE based approach, all stored data files are encrypted using the same key. This is not a sound security design since the more we use a key, the more information the attackers can obtain to break the key. We therefore need to update the key frequently enough to avoid the key wear-out.

3) None of the relavant works [14],[15] were abale to hide the access pattern.The only SSE sheme that hide access pattern are propsed by ostrovsky [16]. His methods were based on oblivious RAMs and are highly inefficeint due to the round complexity.

We take a heuristic approach instead of hiding the search and access patterns instead of relying on relatively heavy cryptographic techniques. Our proposed pattern hiding scheme just slightly increases the computation and storage costs at the public cloud compared to the most efficient construction

B. Health record access privacy and auditability using attribute based encryption (ABE)

The second component is the data access during emergencies where the EMT requests data through the private cloud. The proposed approach is for the general data access, although we focus on the emergency access since it is more challenging. The emergency access supported by Zhang [13] is based on a personal device which is subject to theft, loss, or dead battery, and cannot meet the requirement of anytime anywhere accessibility.

Several papers which are most relevant to our model have followed the approach to define a set of attributes for each single data file [17]. Each file is then directly encrypted under the associated attributes by ABE [17] or encrypted by a different key which is in turn encrypted under the attributes by ABE. There are various limitations of this approach.

First of all, users are not in a good position to determine who needs access to which data files. This is one of the most prominent features of health data access which requires flexibility and professional judgment. Second, the authenticity of the attributes cannot be verified which is a very practical problem and highly challenging in the proposed mobile health networks, where a set of attributes is defined for each general role that will access that data. Third, using the ABE-based access control alone cannot audit who has accessed which data. ABE serves as a gatekeeper to prevent unauthorized parties from decrypting the data. However, it does not provide any mechanism for auditability, i.e., to record and prove that an authorized party has accessed certain data. Without auditability, it is not possible to identify the source of breach if authorized parties illegally distribute the health data.

To overcome these difficulties, we propose to combine threshold signature with ABE-based access control. A(k, n) threshold signature [18] guarantees that a valid signature on a message can be generated as long as there are k valid signature shares. For instance, we can set n = 5 representing the private cloud, the primary physician, the EMT, the specialists (e.g., pediatrician and urologist), and the insurance provider. The private cloud and primary physician are fully trusted by the user.

In our design, users do not encrypt their health data using ABE. The health data is encrypted using the very efficient method described in our storage privacy component. Instead, users use ABE to encrypt the secret shares so that only authorized parties can decrypt them and generate valid signatures. The private cloud and EMT will threshold-sign the data access request submitted by the EMT which contains the keywords and time range the EMT wishes to search. The user can check the request and the validity of the threshold signature to audit the following at a later time

C. Efficient key management using pseudo randomnumber generator for unlinkability

Pseudo random number generator based on cryptography is not truly random but deterministic in nature, it creates a numbers that are sufficiently random for enhancing security mechanisms.

In our design, we use file identifiers that will appear random so that adversaries cannot link multiple stored files to a same user. In this scheme the system will use the function PRF (pseudo random number function).The private cloud will pick (a, b, c, η), each of them serves as a key for either a pseudorandom function (PRF). The private cloud inputs a secret seed η into the PRF and obtains two outputs _ = PRF(η, 1) and ν = PRF(η, 2). The outputs _ and ν will be used as the seeds for generating the update keys sf and the file identifiers fid, respectively. Specifically, fid = PRF(ν, k), $1 \le k \le |F|$, where |F| denotes the number of data files in the collection F. The first node Li,1 is addressed by addri,1 . The pointer ptr indicates the index location in A[*] and is the output of a pseudorandom permutation prpa () computed from the private cloud's secret a. Similarly, prp_ c () is another PRP computed from the secret c for index location of T[*]. The keyword is encrypted by a pseudorandom function prfb () computed from the secret b.

VII. BENEFITS OF EHR

In this digital world, electronic health record (EHR) has significant merits. Several of them are as follows:

- EHR has the ability for efficient storage and retrieval.
- EHR can share updated information among different organizations.
- EHR allows emergency medical technicians (EMT's) to store patient's health record and retrieve it at the time of emergency.
- EHR is stored and maintained in such a way that less redundancy of efforts is required.
- The overall cost for medical systems gets reduced once implementation is complete.
- EHR has the ability to share patient's record which is in the form of multimedia like medical imaging results, forensics.

VIII. CONCLUSION AND FUTURE WORK

By using the cloud computing platform in healthcare system may considerably improve the access to information, which can be done faster and easier. In this paper, we reviewed some the existing works on cloud-assisted electronic health record and maintenance. The paper puts light on various system models based on cloud for e-health data. We have also discussed various methods for enhancing privacy preserving data storage, auditability and efficient cryptography based key management technique using pseudo-random number generator for unlinkability. We have also depicted the use of combined key management technique called as elliptic-curve Diffie-Hellman (ECDH) which is more efficient being having smaller key size than RSA, pseudo-random number generators or than any other technique, so it is considered as a future work

REFERENCES

[1] U.s Depaetment of health & information service, "Breaches affecting 500 or more individuals ". Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

[2] G. Clifford and D. Clifton, "Wireless technology in disease management and medicine," Ann. Rev. Medicine, vol. 63, pp. 479–492, 2012.

[3] R. Curtmola, G. Ateniese, B. de Medeiros, and D. Davis, "Medical information privacy assurance: Cryptographic and system aspects," presented at the 3rd Conf. Security Commun. Netw., Amalfi, Italy, Sep. 2002.

[4] & Winandy, Hans, L., Sadeghi,A.M securing E-health cloud. 1st International informatics symposium 2010.

[5] Liang, X. Barua, M, Enabling security and patient-centric access control for E-health in cloud computing. Int J. Security and networks, Vol.1 IEEE INFOCOM'!!-SCNC, 2011

[6] C.-D. Lee and W.-B. Lee "A cryptographic key management solution for HIPAA privacy/security regulations," IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, Jan. 2008.

[7] on the Duality of MPL Representatives," Proc. IEEE Symp. Computational Intelligence in Scheduling (SCIS 07), IEEE Press, Dec. 2007, pp. 57-64, doi:10.1109/SCIS.2007.357670.

[8] C. Zhang, L. Guo, J. Sun, and Y. Fang, "PAAS: Privacy-preserving attribute-based authentication system for eHealth networks," in Proc. IEEE Intl. Conf. Distrib. Comput. Syst., Jun. 2012, pp. 224–233.

[9] Terry, Gunter, D. Nicolas P. The Emergence of National electronic health record architectures in the United States and Australia Journal of Medical Internet Research 7 (1), 2005

[10] K. Ren, M. Li, S. Yu and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," SECURECOMM'10, pp. 89–106, 2010

[11] E. Horvitz, J. Benaloh, M. Chase, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronicmedical records," in Proc. ACM Workshop Cloud Comput. Security, 2009, pp. 103–114.

[12] Steve, G. Cloud Computing, Oxford University, England, International journal of Innovative Research in Engineering and Science, 1(1), ISSN 2319-5665,

[13] J. Sun, X. Zhu, C. Zhang, andY. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.

[14] E.-J. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol. 2003,p. 216, 2003.

[15] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," presented at the ACM Conf. Comput. Commun. Security, Alexandria, VA.

[16] R. Ostrovsky, "Efficient computation on oblivious RAMs," in *Proc. ACMSymp. Theory Comput.*, 1990, pp. 514–523.

[17] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and Secure Sharing of Personal Health Records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.