Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-4, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Privacy and Protection of Mobile Health Data on Secure Cloud Storage

Naseeruddin Ali, Naziya Pathan, Shyam P. Dubey
Research Scholars, CSE, NCOET Nagpur
Assistant Professor, CSE, NCOET Nagpur
H.O.D, CSE, NCOET Nagpur

Abstract*: Inspire d by security issues in electronic healthcare systems which has been a vast success on cloud platforms, we propose to build security in mobile healthcare systems with the help of private cloud. Today, communication and information technology are becoming an integral part in healthcare. The system offers mechanism for privacy-preserving data storage and retrieval. Retrieval is most helpful at the time of emergencies. The system also offers auditability for misusing health data. We have integrated attribute based encryption with threshold signing for providing security and symmetric searchable encryption for providing search over encrypted documents to owner.*

1. Introduction

The electronic health care systems are dominantly growing 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 (http://www.hhs. gov/ocr/privacy/hipaa/administrative/breach notification rule/ breachtool.html), around 9 million patient's health record was leaked in past three years. Even though 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 algorithm s in mobile health monitoring (Clifford and Clifton, 2012) which is cloud based was considered future trend. In the past, information about patients, the illness 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 disadvantage of trivial file system was that files misplaced 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 overall 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 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 leading 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 all along gathering data. 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 ensure the privacy and security to stand as a guard against the adversaries and possible threats. The cloud-assisted service model supports the implementation of practical privacy mechanisms after all intensive computation and storage can be shifted to the cloud, leaving mobile users with lightweight tasks.

2. Related Work

As far as emergency medical services are concerned, the earliest works to perform on e-healthcare is medical information privacy assurance (MIPA) (Curtmola et al., 2002). It was one of the few works that indicate the important challenges for privacy of medical data. It has also put on lights on devastating privacy breaches that were caused by inefficient technology. MIPA developed privacy-protecting infrastructures and technology to simplify the personalized development of health information. Terry and Gunter (Terry et al., 2005) 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 become handy in assuring data is accurate, appropriate and legal. It has significantly reduced the chances of data duplication as there is only one modifiable file, which means that the file is updated regularly when explore at a later date or day and removed the issue of lost forms or paperwork.

The concept of patient controlled encryption (PCE) was proposed by Horvitz et al. (2009) 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. The cryptographic key-management solution for e-healthcare systems was proposed by lee and lee (Lee and Lee, 2008) 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 (SCIS, 2007) proposed framework for privacy-preserving attribute-based authentication system in e-health networks. The attribute-based authentication schemes designed for higher privacy levels sustain the more privacy on attributes and attribute values, but cost more computation and communication resources.

Winandy and colleagues (2010) have revealed 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. Ren and colleagues (2010) 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 accessing 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. Liang (2011) and colleagues proposed efficient and patient-centric access control scheme which allows data requester to have different access privileges which is termed as role-based access, and then assigns different related attribute sets to them. Performance analyses and extensive security mechanisms and demonstrate that the scheme is able to achieve targeted security requirements with little amount of communication delay.

3. Proposed Plan

3.1. System Model

Our system proposed two applications for mobile users, who can be either patient or Hospital Staff (Doctor).

- Emergency Medical System (EMS) for users
- EMS Admin for Owners

Users collect their health data through the monitoring devices they carry carried. Emergency medical system (EMS) Admin is a physician who performs emergency treatment. The computing facilities are mainly mobile devices carried around such as Smartphone, tablet, or personal digital assistant.

Every user is correlated with one private cloud. Multiple private clouds are supported on the same physical server. Private clouds are always online and available to handle health data on behalf of the users. This can be very adorable in situations like medical emergencies. The private cloud will process the data to add security protection before it is stored. We assume that at the bootstrap phase, there is a secure channel among the user and his/her private cloud, e.g., secure home Wi-Fi network, to negotiate a long-term shared-key. After the bootstrap phase, the user will send health related information over insecure network to the private cloud residing via the Internet backbone.

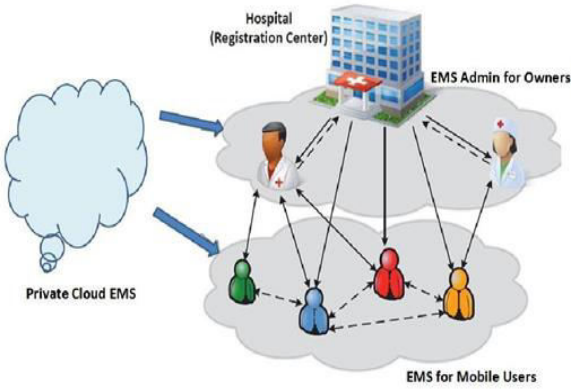

Figure 1: Cloud-assisted Mobile Health Network for Users & Admin

3.2. Threat Model

The private cloud is fully trusted by the user to finalized health data-related computations. Public cloud is considered 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 record. The doctors are granted access rights to the health record only pertinent to the treatment, and only when emergency takes place.

4. Materials and Methods

In this section we introduce framework and methods for privacy preserving data storage on clouds. The system offers two schemes as follows.

4.1. Attribute-Based Encryption (ABE) with Threshold signing

ABE was proposed by Sahai and Waters (2005). In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In Key-policy ABE or KP-ABE (Goyal et al, 2006), the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is capable to decrypt information if it has matching attributes. In Cipher text-policy, CP-ABE

(Bethencourt et al., 2007), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates. ABE-based access control individual cannot audit who has accessed which information. 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 user has retrieved certain information. Without auditability, it is not possible to identify the source of breach if authorized parties illegally distribute the health data. In our use of ABE, the user (and his/her primary physician) will have no clue about whether an authorized party has properly accessed the data without auditability. To overcome these difficulties, we propose to combine threshold signature with ABE-based access control. A(k, n) threshold signature (e.g., (41)) 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 completely trusted by the user. Let k = 2 such that any not fully trusted party must meet the threshold signing with either fully trusted party. In reality, for example, the EMS Admin better performs the signing with the private cloud because the primary physician may not be present online at all times. On the other hand, a pediatrician better performs the signing with the primary physician since users normally rely on their primary physicians for referral to a specialist. The user secret shares a key to n participating parties.

1) User labels some parameters for ABE-controlled threshold signing. Let H: {0, 1}* → G be a hash function. Let G1 be a bilinear group of prime order p1, g and g1 be generators of G1 and e: G1 × G1 → G2 be a bilinear map.
2) User (k, n)-shares x such that any subset S of k or more can reconstruct x using the Lagrange interpolation: x = Ei∈ SLixi where Li are the appropriate Lagrange coefficients for the set S and xi are the secret shares.
3) User ABE-encrypts the secret share xd for EMT, indicate by ABE(xd), as: Define the universe of attributes U = {1, 2, . . . , u} and a hash function h : {0, 1}* → G2 .Randomly choose a number vj∈R Zp1 for each attribute j ∈ U and a number z ∈R Zp1. The public parameters are V1 = gv1 1,. . . , Vu = g1vu, Y = e(g1, g1)z , and the master secret key is (v1, . . . , vu, z). Obtain the encrypted share for EMS Admin as ABE (xd) = (_, xdYτ, {Vτ j}j∈ _), where _ is a set of attributes and τ∈R Zp1 is a randomly chosen secret value.
4) User generates the decryption key D for EMT using the ABE key generation algorithm and sends (ABE(xd), IBERole(D)) tothe private cloud, where IBE Role is the IBE using the general role ole = EMS Admin as the public key.
5) When EMS Admin requests medical data from the private cloud, EMS Admin sends the attributes _, the attribute certificate (_) SIG, and REQ which contains the keyword for search and the time range of interest. The private cloud verifies_ using (_)SIG and returns (ABE(xd), IBERole (D)) to EMS Admin.EMS Admin first decrypts for D using the private key corresponding to the role "EMT," and then decrypts for xd using D.
6) Private cloud and EMT each generates partial threshold signatures σ i = (H (REQ)) xi, and exchange σ i and yi = gxi. They verify the partial signature from each other by checking if (g, yi, H (REQ), σ i) is a valid Diffie–Hellman tuple.
7) Private cloud and EMT generate the threshold signatureσ = _i∈S (σLi i) which can be verified by anyone bychecking if (g, y,H(REQ), σ) is a valid Diffie–Hellman tuple. The private cloud stores ói from EMT, ó, REQ, and the date/time request is made.

The computational load on the mobile user is light since secret sharing needs to be performed once and for all, and the ABE encryption of the shares needs to be performed only for a limited number of general roles.

4.2. Searchable symmetric Encryption (SSE)

The cloud-based electronic health record and its model composed 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 such that storage privacy and efficient retrieval can be carried out. Next Privates cloud involves in auditability scheme with users. 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. The Second application EMS Admin uses efficient searchable symmetric encryption (SSE) which provides the search over encrypted health data. With first module EMS, the users store their health record on public cloud in encrypted form using ABE. And next with EMS Admin module where hospital staff or doctors can search over that encrypted data using SSE. We begin by reviewing the formal definition of an index- based SSE scheme. The participants in a single-user SSE scheme include a client that wants to store a private document collection D = (D1, . . . ,Dn)

on an honest-but-curious cloud server in such a way that the server will not learn any useful information about the collection. We consider searches to be over documents.

An index-based SSE scheme over a dictionary Δ is a collection of five polynomial-time algorithms SSE = (Gen, Enc, Trpdr, Search, Dec) such that,

1) K ← Gen (1k): is a probabilistic key generation algorithm that is run by the user to setup the scheme. It takes as input a security parameter k, and outputs a secret key K.
2) (I, c) ← Enc (K, D): is a probabilistic algorithm run by the user to encrypt the document collection. It takes as input a secret key K and a document collection D = (D1, . . . ,Dn), and outputs a secure index I and a sequence of ciphertexts c = (c1, . . . , cn). We sometimes write this as (I, c) ← EncK(D).
3) t ← Trpdr(K, w): is a deterministic algorithm run by the user to generate a trapdoor for a given keyword. It takes as input a secret key K and a keyword w, and outputs a trapdoor t. We sometimes write this as t ← TrpdrK(w).
4) X ← Search (I, t): is a deterministic algorithm run by the server to search for the documents in D that contain a keyword w. It takes as input an encrypted index I for a data collection D and a trapdoor t and outputs a set X of (lexicographically-ordered) document identifiers.
5) Di ← Dec (K, ci): is a deterministic algorithm run by the client to recover a document. It takes as input a secret key K and a ciphertext ci, and outputs a document Di. We sometimes write this as Di ← DecK(ci).

An index-based SSE scheme is correct if for all k ∈ N, for all K output by Gen(1k), for all D ⊆ 2 Δ, for all (I, c) output by EncK(D), for all w ∈ Δ, Search I, TrpdrK(w) = D(w) ^ DecK(ci) = Di , for 1 ≤ i ≤ n.

5. Experimental Work

In this section, we give snapshots of various modules mentioned in this paper. We begin with the first module which Emergency Medical System (EMS). Using EMS, patient stores the complete health record on private cloud in encrypted form. The encryption is done using attribute based encryption (ABE).

Figure 2: Patient's Health Record

The above figures show the snapshots of EMS application. Figure 2 shows the health record of patient consisting various information like personal info, allergies, medications etc. The whole record is entered and stored by user on private cloud. The health record is encrypted with the help of attribute-based encryption (ABE).

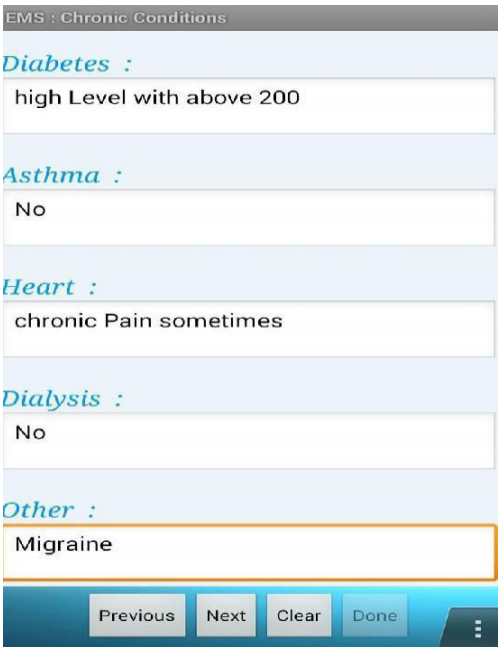

Figure 3: Chronic Conditions

Figure 3 shows the chronic conditions of patient and the disease they are suffering from.

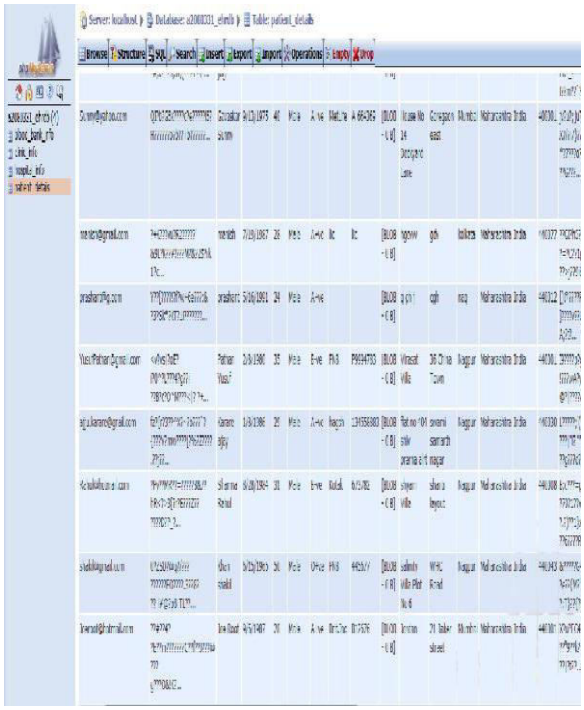

Figure 4: Patient's Health Record on Private cloud

Figure 4 shows the electronic health record of patient on private cloud. The private cloud is honest but curious so the health record is stored in encrypted using ABE to provide privacy. In figure all the fields are not encrypted in order to differentiate between encrypted and unencrypted data. However in working scenario all the fields are in encrypted form. Now we begin with the next module which is EMS Admin. This application is basically used by the medical technicians in hospital who provide emergency services to patients. Admin is connected with private cloud and retrieves the health data from cloud which is in encrypted form. The EMS Admin provides search over encrypted data using SSE.

Figure 5 shows the health data maintained by medical technicians to provide emergency services to patients. The admin conceive the data and stores it on private cloud. The details of hospitals are added and which emergency service provided by that hospital are added. The location of that hospital (latitude and longitude) is added so that navigation service can be used using Maps.

Figure 6 shows emergency services provided by the hospital. All this data is added by the EMS Admin. One or all emergency service can be selected by medical technician. Emergency services are like heart attack, accidental cases, poisoning etc. For every type of emergency EMS admin prepares the health data and stores it on private cloud through which users and doctors are connected.

Figure 5: Hospital Record by Admin

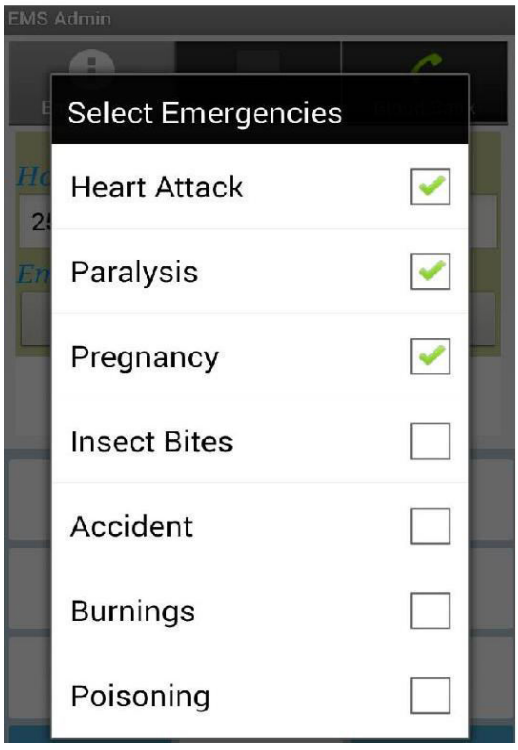

Figure 6: Emergency Services

Figure 7: Emergency Services Selection of Hospital

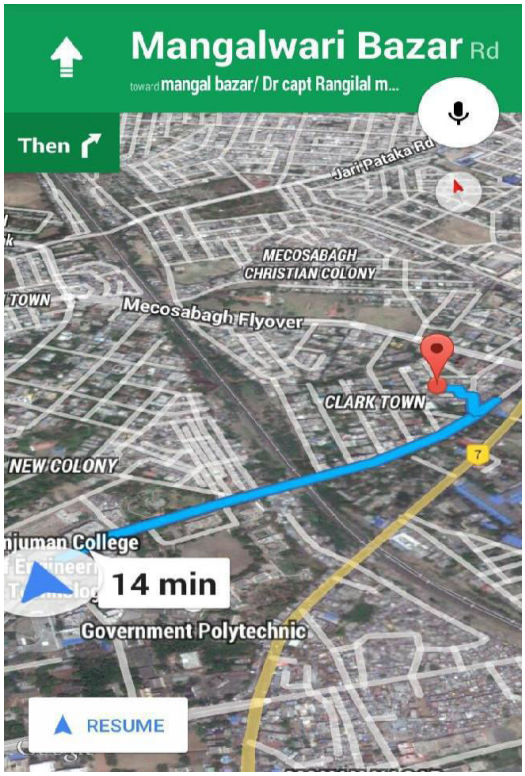

Figure 8: Location of Hospital

Figure 7 shows the list of hospitals which match to the emergency services selected by the user. Figure 8 shows the hospital selected by user. The user can get the directions of selected hospital and can navigate using Google Map.

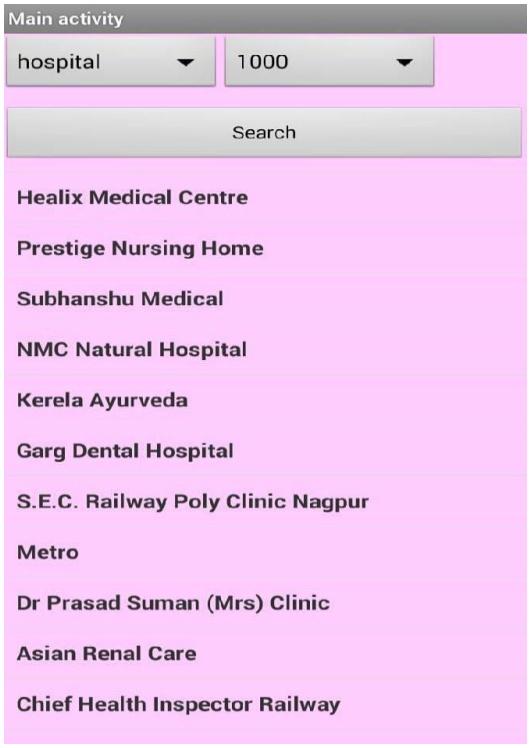

Figure 9: Anonymous Google search for Hospitals

Figure 9 shows the anonymous search for the hospitals using Google's database. This search is not admin oriented which means that user will use the services of Google database and maps to find the locations of hospitals nearby. The user can enter the range of kilometers in order to search for the hospital or clinic. Both EMS and EMS Admin module are mobile applications which are configured in user as well as medical technician's tablet, mobile phone or PDA's. Both the applications are connected with private cloud where data is stored and retrieved in encrypted form.

Attribute-based encryption (ABE) is used which is suitable where data is in the form of files. The EMS database is nothing but the Sqlite database which is file based. That is why we opted out for the ABE. Searchable symmetric encryption (SSE) is used by EMS Admin module to provide the search over encrypted documents. Whole health record id stored on private cloud in encrypted form and EMS Admin searches over that encrypted data to provide privacy preserving data storage and auditability.

6. 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. This paper focuses on privacy of healthcare system which we have deployed using cloud computing technology. We proposed to build privacy into mobile health systems with the help of the private cloud. We provided solution for privacy-preserving data storage by integrating attribute-based encryption (ABE) with threshold signing and efficient key management. We have also used symmetric searchable encryption (SSE) to provide auditability and search over encrypted documents to owners. We have shown the insights into the modules. We reviewed some the existing works on cloud-assisted electronic health record and maintenance. We have also discussed various methods for enhancing privacy preserving data storage, auditability a 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.

7. References

[1]. Bethencourt, J., A. Sahai, and B. Waters, 2007. "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy. , pp. 321–334.

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

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

[4]. Curtmola, R., 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.

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

[6]. Goyal, V., O. Pandey, A. Sahai, and B. Waters, 2006. "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, pp. 89–98.

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

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

[9]. Li, M., S. Yu, Y. Zheng, K. Ren, and W. Lou, 2013. "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.

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

[11]. 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.

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

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

[14]. Sahai,A. and B. Waters, 2005. "Fuzzy identity-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 3494. Springer, pp. 457–473.

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

[16]. U.S Department of health & information service, "Breaches affecting 500 or more individuals". Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breac hnotificationrule/breachtool.html.