Privacy Preserving System Using Attribute Based Encryption for e-Health Cloud

Kushal P. Kulkarni[1], Arati M.Dixit[1, 2]

[1]Department of Computer Engineering, PVPIT/JSPM, Bavdhan, Pune, Maharashtra, India

[2]Department of Technology, Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract: ***Cloud computing is generally a distributed computing over a network. It plays an important role in healthcare integration costs, optimizing resources in a new era of innovations. Many healthcare providers and insurance companies today have adopted some form of electronic medical record systems, most of the medical records stored in centralized databases in the form of electronic records. Typically, a patient may have many healthcare providers, including primary care physicians, therapists, physicians and other medical practitioners. Patient may use multiple healthcare insurance companies for different types of insurances, such as medical, dental, vision, and so forth. Sharing of personal medical records is a patient centric model of health information exchange which can be stored at third party such as cloud providers. The confidentiality of the personal health records is major problem when patient uses commercial web based systems to store their health data, because it can be viewed by everyone. Providing privacy for their own medical records is a promising method to encrypt the files using various cryptographic approaches. There are various issues such as risks for privacy of records, scalability in key management and flexible access have the most important challenges towards achieving fine grained and cryptographically data access control. To achieve fine-grained and scalable data access control for PHRs, we uses attribute based encryption (ABE) techniques to encrypt each patient's medical record file. This survey describes new approach for secure storage and controlled sharing of patient's health data.***

Keywords: E-health Cloud, Cloud Computing, ABE Techniques, PHR, Data confidentiality

1. Introduction

The costs of healthcare services rise and healthcare professionals are becoming hard to find the information then healthcare organizations are concerned with health information technology (HIT) systems. HIT allows health organizations to provide services in a more efficiently and cost-effectively manner. Technologies such as Cloud Computing (CC) provide a strong infrastructure and offer HIT services over the Internet. This can be achieved by a pay-as-you-use model of the "e-Health Cloud" to help the healthcare industry cope with current and future demands yet keeping their costs to a minimum. Over the past three decades, computer systems are used extensively in medical and healthcare systems. For the documentation, storage, processing, analysis and presentation of patient's information storage devices and server systems are used in developed countries today. Most healthcare systems are built on the basis that consists of paper medical records, handwritten test results, digitized and non-digitized images, and handwritten notes. Sharing of information across providers is inefficient and insecure and portability of data is very rare [1]. All these processes are time consuming. So, there exist many more challenges in this sort of systems where a large number of records are stored and data requirements are scalable, flexible, and easy to create, update, manage and access etc. but security has topmost priority.

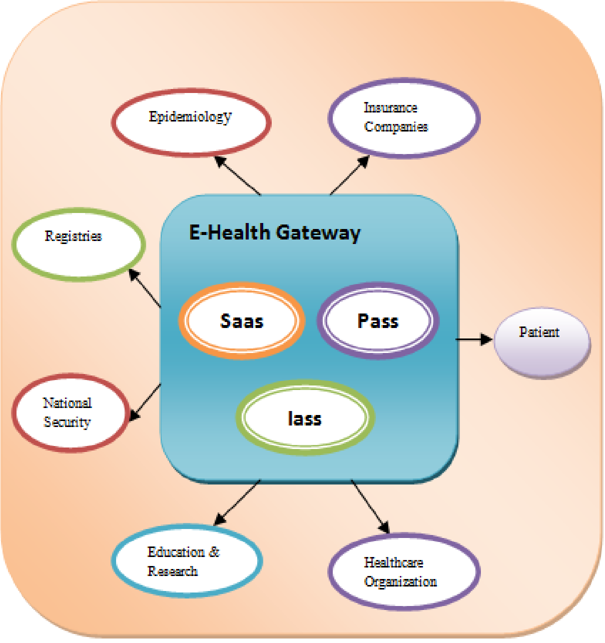

Figure 1: Generic Architecture of e-health cloud

e-Health Cloud as presented in Fig. 1 is a Cloud that provides IT services to improve patient's efficiency. Typically, the Cloud consists of an array of layered structure, starting with the basic physical layer of storage and server infrastructure and working up through the application and communication layers. The e-Health Cloud can be divided into different implementation models based on whether it is created internally (private Cloud), outsourced (public Cloud) or a combination of the two (hybrid Cloud).Cloud-based HIT solutions used for patients, healthcare providers, and other concerned organizations such as research facilities and insurance companies and. The e-Health Cloud concerned with a Gateway and Service-Based Applications.

Gateway: This component can be set to perform several important tasks: (i) managing access to the Cloud (ii) verifying EHR (Electronic Health Record) provided by different health care providers in terms of integrity, authenticity, confidentiality and security with medical data exchange (iii) combining and integrating EHR data into a new Cloud-based EHR; (iv) selecting and de-identifying EHR to share with the public Cloud for research, educational and industrial purposes [2]. Service Based Applications such as services for national security and epidemiology, Web Portal, Picture Archiving, registries and Communication Systems (PACS); all of which provided as services that are easily managed through CC operational parameters. Software as a Service provides Cloud-based software solutions (e.g., clinical systems i.e.CSM) where consumers such as healthcare providers or financial and insurance brokers receive access to the software capabilities of the cloud. Platform as a Service extends the basic infrastructure with High-level integrated environment to design, build, test, deploy and update online healthcare applications. Infrastructure as a Service deals with the physical processing and storage resources.

Various mechanisms have been developed to preserve and improve privacy of the e-Health systems in the cloud computing. We presents an overview of the privacy preserving cloud health record system using attribute based encryption approach that have been used in the e-Health clouds. A Personal Health Record (PHR) service allows a patient to create, manage, and control her personal health related data in one place through the web, which makes storage, retrieval, and sharing of the medical information in efficient manner. Especially, each patient is having the full control of her medical records and can share their health data with a wide range of users, including healthcare physicians, family members or friends. Due to the high cost of building and maintaining specialized and equipped data centers, most of the PHR services are provided by third-party service providers, for example, Microsoft Health Vault. The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either access the PHR for personal use or professional uses. Examples are close friends and family member while the latter can be medical doctors, pharmacists, and researchers, etc. We refer the two criteria's of users as personal and professional users, respectively. Each owner is responsible for managing all the available professional users by the key management. In Existing system a PHR system model, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Every user obtains keys from each owner whose PHR she wants to read would limit the accessibility since patients are not always online. The rest of the paper is organized as follows. Section II discusses the Technical and non-technical challenges facing e-Health Cloud. Section III presents concept of Attribute based Encryption Technique. Overview of the privacy preserving approaches used in the cloud based health record systems i.e. PHR are presented in Section IV and Section V concludes the discussion and highlights the open research issues and areas.

2. Related Work

Several works has been attempted to implement the concept of PHR maintenance system. Ming Li Shucheng Yu, Yao Zheng, [28] presented approach of the secure sharing as well as Revocable Attribute Based Encryption and scalability of the users and explains how public key cryptography used with the ABE as well as Fine Grained Access Control. Y.Zheng discusses the master thesis for the preserving the privacy of public health records in cloud computing and gives the good understandable idea about the privacy of the health records to maintain in the cloud. Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi highlighted opportunities and challenges of e-health Cloud [27]. S. Yu, C. Wang, and W. Lou, provides the data sharing based on attribute and revocation based on attributes [22]. Ibraimi et al., has proposed secured method on PHR by applying attribute-based Encryption, as it provides a secure Methodology [30]. This method does not rely on a central authority to grant the key to the social or professional users. This method provides access rights to the owner of the PHR. CP-ABE scheme is used in this system. S. Narayan, M. Gagne´, and R. Safavi-Naini, provides the preserving the privacy of the Electronic Health Records system with the use of the Attribute Based Infrastructure [23].Liang et al. [24] proposed a self-controllable access policy for the patients so that they can have easily access to their PHI (Personal Health Information). But this sometimes causes the whole system unsecured. Sun *et al.* [31] studied Privacy-preserving health data storage, where patients encrypt their own health data and store it on a third-party server.Yu et al. [25] well defined access structure policy based on KP-ABE for managing and storing data in the cloud. Privacy and confidentiality of patient's information and use of secret key for accessing data from the cloud are guaranteed in this kind of system. Besides, many of research works have shown that use of fragmentation after encryption on data makes the data more reliable and improves the system's overall performance as potential intruders always. Author [26] presented the excellent technique for accessing the data i.e. Fine Grained Access Control with the Multi Owners for accessing the records and provides the scalability for the users for accessing the records.

3. Challenges of E -Health Cloud

1. Technical Challenges

a. **Interoperability:** The issue of interoperability is also faced when integrated e-Health Cloud services are provided from both local and external clouds. One approach is to use the concept of Service-Oriented Architecture (SOA) [18] for implementing the e-Health Cloud.
b. **Availability:** Most healthcare providers require high availability of the e-Health Cloud services. Service and data availability is crucial for healthcare providers who cannot effectively operate unless their applications and patients' data are available. The e-Health Cloud services should be available continuously with no interruptions or performance degradation [16].
c. **Scalability:** Many healthcare providers with millions of patient records could be handled by an e-Health Cloud, which is only achievable if and only if the

services provided are scalable. Cloud scalability is mainly enabled by increasing the capacity and number of IT resources such as compute nodes, network connections, and storage units and providing suitable operational and management facilities.

d. **Data/Service Reliability**: All e-Health Cloud services and data must be error-free. Some important decisions regarding single human or society health can be taken depending on the data and services provided by the e-Health Cloud. As such services are distributed and may come from a number of Cloud providers, the chance of having faulty or incorrect data or services can increase.
e. **Flexibility: A**n e-Health Cloud must be capable of serving multiple healthcare providers [15] with different requirements. These requirements are in terms of functions, operations, users, auditing, management, and quality of service (QoS) requirements. The e-Health Cloud should be very flexible in adding new needed services to support healthcare processes.
f. **Data Management:** Huge numbers of medical records and images related to millions of people will be stored in e-Health Clouds. The data may be repeated for high reliability and better access at different locations and across large geographic distances. Most medical applications require secure, efficient, reliable, and scalable access to the medial records. These requirements enforce the need to have some storage services that provide fault tolerance, secure storage over public clouds, and rich query languages that allow efficient and scalable facilities to retrieve and process the application data.
g. **Security:** High security concerns are usually associated with open environments which are provided by a number of service providers and shared among a number of service consumers.. That is essential since data must be kept secure in the clouds where it is stored along with other healthcare providers' data.
h. **Privacy**: privacy is an important issue that could prevent the full utilization of its capabilities for different types of organizations and applications [18,19]. The concerns involve the ability to protect patient's records from each other, other healthcare providers and the cloud service providers.

2. Non-Technical Challenges

a. **Organizational change:** E-Health Cloud will require significant changes to clinical and business processes and also to the organizational boundaries in the healthcare industry. Examples of such changes could be in the form of new policies, procedures and workflows in addition to changes in how medical processes and documentation are done.
b. **Legislations and standards:** there are still no clear or adequate legislations and guidelines for clinical, technical and business practices of healthcare in the e-context. This includes the lack of standards for medical informatics, policies, inter-operability, and transmission methods in e-Health Cloud. Currently, there are some standards and classifications for health information systems in general some of which can be adopted for the e-Health Cloud. One example is the International Classification of Diseases tenth revision (ICD-10) issued by the World Health Organization (WHO). It defines a medical classification list for the coding of diseases, signs or abnormal findings, complaints, social conditions, and external causes of injury or diseases. Another classification is The Systematized Nomenclature of Medicine (SNOMED) which was designed as a detailed categorization of clinical medicine for the purpose of storing and/or retrieving records of clinical care in human and veterinary medicine [20].
c. **Ownership of Data:** Data ownership in the industry health in general is an area with no clear guidelines. This challenge is concerned with the creation of policies and guidelines that draw clear ownership boundaries.
d. **Usability and users experiences:** This challenge is concerned with the degree and level of adoption obtained by the e-Health Cloud users including patients, healthcare professionals, and administrative and insurance personnel. Proper and adequate pre-implementation training and marketing along with continuous post-implementation training are important to help overcome this challenge.
e. E-Health Cloud provides valuable benefits to the health care industry; it extends the major challenges of HIT and CC together and adds more weight to these challenges as it is used to store and process sensitive medical data. Here we summarize the technical [3-9] and non-technical [3,4,10-15] challenges particularly faced by the e-Heath Cloud.

4. Attribute Based Encryption Techniques

At the early stages of the cloud computing and personal health record the traditional encryption techniques were applied to the personal health record and now days the advanced encryption techniques such that attribute based encryption and its different variations are used.

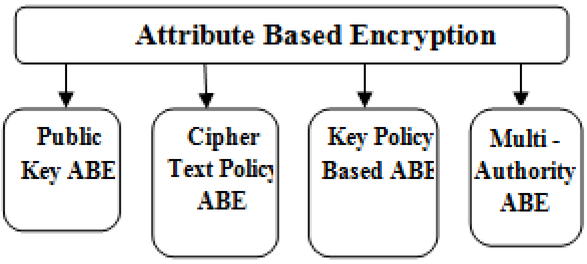

Figure 2: ABE Techniques

4.1 Attribute Based Encryption

Attribute-based encryption (ABE), one of most preferable identity-based cryptographic systems where attributes are taken as input and cryptographic operations are done on those attributes based on defined policies. Using ABE technique we are providing security to the database. In this the sensitive information is shared and stored in the cloud provider; it is needed to encrypt cipher text which is classified by set of attributes. A. Sahai and B. Waters provide the initialization of Attribute Based Encryption as well as detailed about the Fuzzy Identity Based Encryption techniques [21]. In this system both the cipher text and secret key will be associated with the attributes. The user who is having a minimum number of attributes only can decrypt the data.

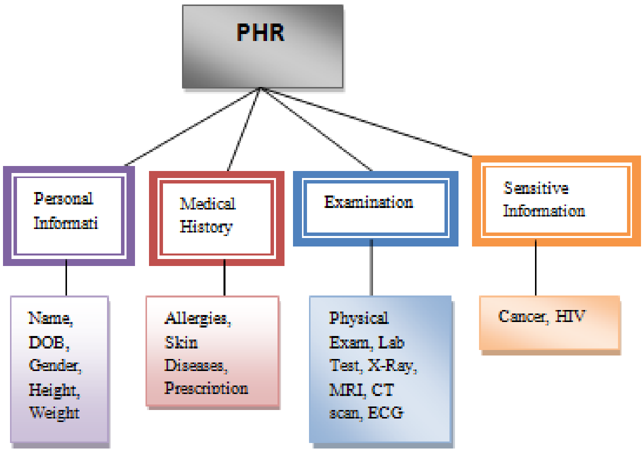
PHR
Personal Informati
Medical History
Examination
Sensitive Information
Name, DOB, Gender, Height, Weight
Allergies, Skin Diseases, Prescription
Physical Exam, Lab Test, X-Ray, MRI, CT scan, ECG
Cancer, HIV

Figure 3: Attribute Hierarchy of health records

Public key encryption was the most traditional method applied to the PHR for the security of the data. But it made the high key-management problems and also this method was very less scalable. Cipher text Policy Attribute based Encryption (CP-ABE): technique is used to keep encrypted data confidential The key-idea of the CP-ABE is: the user secret key is associated with a set of attributes and each cipher text will embedded with an access structure. The user can decrypt the message only if the user's attribute satisfied with the access structure of the cipher text [22].

Key-Policy Attribute-based Encryption (KP-ABE) is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet. The KP-ABE is useful for providing the fine-grained access control to the data system where it can efficiently specify that which part of data system can be accessed by which user and what are the operations they can execute over there. Multi-Authority Attribute-Based Encryption (MA-ABE) is an advanced attribute based encryption in which it concerned with multiple attribute authority for handling the different set of users from different domains. [23] In the PHR system the users will be from different domain like the doctors from health care organizations, the friends and family from personal relations and other users from insurance domain too. Thus the MA-ABE scheme will highly reduce the key-management issues and it will provide fine-grained access control to the system.

4.2 Proposed PHR System

Traditional clinical settings concerned with paper-based medical records and prescriptions have also advanced to the Personal Health Records (PHRs) and the Electronic Health Records (EHRs).From the clinical point of view, it is important to access the up-to-date integrated patient health information. E-health cloud can be considered as a platform that, besides storing huge volumes of the health data, also serves as a structured management of the health data across multiple healthcare providers. In the existing system the data owner is uploading the data to the cloud server, after encrypting the data according to the access control policy [29] defined with the set of attributes. This encrypted data can be decrypted by the user only if the attributes of that user satisfies the access control policy. The problem addressed here is the confidentiality of PHRs. Patients records contains sensitive information such as details of a patient's disease, drug usage, sexual preferences, etc. Inappropriate disclosure of a record can change patient's life, and there may be no way to repair such harm financially or technically. Therefore, it needs protection for patient's health records when they are uploaded and stored in commercial Web-based systems. Consider following scenario where a patient, has some sensitive personal health records which she wants to store securely in a Web-based PHR, and share them with other users who belong to two different security domains: (1) professional domain (PD) - a healthcare provider group such as doctors, nurses, or (2) social domain (SD) - her family, friends, or patients.

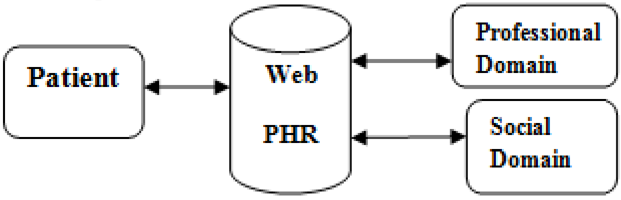

Figure 4: Proposed PHR System Architecture

The scenario gives the idea about the need for a system which fulfills the following security requirements:

a. Protect health records from network attacker. So, data is to be encrypted before it is sent to the web PHR.
b. Health records protected from third parties who store PHRs. The third party manages web PHRs which are not accessible to the plain data.
c. The access policy concerned with the encrypted data, such that only those users having a secret key associated with set of attributes which satisfies the policy might be capable of decrypting it.
d. Users from the professional domain and users from the social domain both need to be properly authenticated and authorized to access the data.

Solution of the problem in the existing system is overcome by the Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. A high degree of patient's privacy is maintained simultaneously with the help of multi-authority ABE. Proposed system enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation a under emergency scenarios. Analytical and experimental results are presented which show the security, scalability and efficiency and privacy of our proposed scheme. Use case diagram of proposed system is shown in the fig:

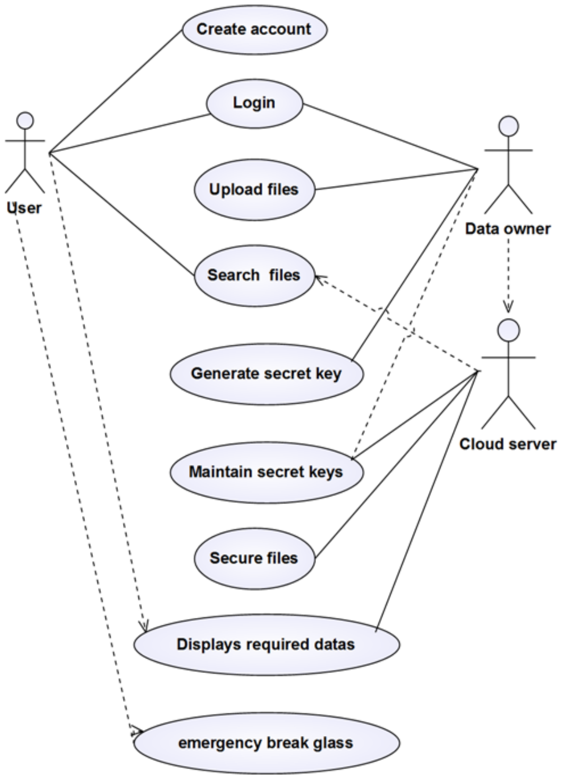

Figure 5: Use Case flow of PHR System

To achieve fine-grained and scalable data access control for PHRs, we adopted attribute based encryption (ABE) techniques to encrypt each patient's health record file We focused on multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users with the help of MA-ABE technique. In this system, we fulfill the mentioned gaps by proposing a security framework model for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users.

5. Conclusion

In this paper, we have proposed privacy preserving and secure sharing patient centric framework for maintaining personal health records in cloud computing. With the help of partially used cloud servers, patients shall full control through encrypting their PHR files to allow fine grained access. This framework concerned with the unique challenges by multiple PHR owners and users, in that we greatly reduce the time, security and complexity of key management. We used ABE technique to encrypt the PHR data, so that patients can allow access as the private users, but not accessible by the public users.

6. Acknowledgement

My sincere thanks to Dr. Arati M. Dixit madam for her helpful opinion and suggestion for the paper.

References

[1] Connecting for Health. The personal health working group final report, 2003 July 1.

[2] AbuKhousa, E.Najati, H.A. UAE-IHC Steps towards Integrated E-Health Environment in UAE. In Proceedings of the 4th e-Health and Environment Conference in the Middle East, Dubai, UAE, 30 January 2012–2 February 2012.

[3] Lohr, H. Sadeghi, A. Winandy, M. Securing the E-Health Cloud. In "Proceedings of the 1st ACM International Health Informatics Symposium (IHI 2010)", Arlington, VA, USA, 11–12 November 2010; pp. 220–229.

[4] Commonwealth Secretariat. Progress report. Available online: http://www.thecommonwealth.org/ files/189921/File Name/HealthProgressReports-E-Health.pdf (accessed on 28 June 2012).

[5] Momtahan, L.Lloyd, S. Simpson, A. Switched Lightpaths for E-Health Applications: Issues and Challenges. In Proceedings of the Twentieth IEEE International Symposium Computer-Based Medical Systems (CBMS'07), Maribor, Slovenia, 20–22 June 2007; pp. 459–464.

[6] Agrawal, D. Abbadi, A. Antony, S.Das, S. Data Management Challenges in Cloud Computing Infrastructures. In Proceedings of the 6th International Workshop on Databases in Networked Information Systems (DNIS 2010), Aizu-Wakamatsu, Japan, 29–31 March 2010.

[7] Hasan, J. Effective telemedicine project in Bangladesh: Special focus on diabetes health care delivery in a tertiary care in Bangladesh. Telemat. Inform. **2012**, 29, 211–218.

[8] Rayport, J.F. Heyward, A. Envisioning the Cloud. The Next Computing Paradigm. A Market space Next Point of View. Available online: http://marketspacenext.com/inthemedia/ envisioning-the-cloud/ (accessed on 28 June 2012).

[9] Introduction to Cloud Computing Architecture. Sun Microsystems, Santa Clara, CA, USA, 2009.

[10] Varia, J. Cloud Architectures. Available online: http://aws.amazon.com/articles/ 1632 encoding UTF8 & jiveRedirect 1 (accessed on 28 June 2012).

[11] Hosseini, A.; Sommerville, I.; Sriram, I. Research Challenges for Enterprise Cloud Computing. Available online: http://arxiv.org/abs/1001.3257 (accessed on 28 June 2012).

[12] Mei, L.; Chan, W.K.; Tse, T.H. A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. In Proceedings of the Asia-Pacific Services Computing Conference (APSCC'08), Yilan, Taiwan, 9–12 December 2008; pp. 464–469.

[13] Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.Rabkin, A.; Stoica, I. Zaharia, M. Above the Clouds: A Berkeley View of Cloud Computing. Available online: http://inst.cs.berkeley.edu/~cs10/fa10/lec/20/2010-11-10-CS10-L20-AF-Cloud-Computing.pdf (accessed on 29 June).

[14] Sriram, I.; Khajeh-Hosseini, A. Research Agenda in Cloud Technologies. In Proceedings of the 1st ACM Symposium on Cloud Computing, SOCC 2010, Indianapolis, IN, USA, 10–11 June 2010.

[15] Youseff, L.; Butrico, M.; da Silva, D. Toward a Unified Ontology of Cloud Computing. In Proceedings of the

Grid Computing Environments Workshop (GCE'08). Austin, TX, USA, 12–16 November 2008; pp. 1–10.

[16] Leavitt, N. Is cloud computing really ready for prime time? Computer 2009, 42, 15–20.

[17] Al-Jaroodi, J.Mohamed, N. Service-oriented middleware: A survey. J. Netw. Comput. Appl. 2012, 35, 211–220.

[18] Nguyen, D.K..Lelli, F. Papazoglou, M.P. van den Heuvel, W.-J. Blueprinting Approach in Support of Cloud Computing. Future Internet 2012, 4, 322–346.

[19] Kelly, E.P.; Unsal, F. Health information privacy and e-healthcare. Int. J. Healthc. Technol. Manag. 2002, 4, 41–52.

[20] Cote, R.A. Architecture of SNOMED Its Contribution to Medical Language Processing. In Proceedings of the Annual Symposium on Computer Applied Medical Care, Washington, DC, USA, 25–26 October 1986; pp. 74–80.

[21] A. Sahai and B. Waters, "Fuzzy Identity-Based encryption," in LectureNotes in Computer Science, vol. 3494, 2005, pp. 457–473

[22] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM International Journal of Communication and Computer Technologies Volume 01 – No.72 Is Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[23] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW'10), pp. 47-52, 2010.

[24] X. Liang, R. Lu, X. Lin, and X. Shen. "Patient self-controllable access policy on phi in healthcare systems", AHIC 2010, Kitchener, Ontario, Canada, pp.1–5

[25] S. Yu, C. Wang, K. Ren and W. Lou, (2010), "Achieving secure, scalable, And fine-grained data access control in cloud computing", INFOCOM, 2010 Proceedings IEEE, San Diego, CA, USA, pp.1–9.

[26] M. Li, S. Yu, K. Ren, and W. Lou, ―Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,‖ Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[27] e-Health Cloud: Opportunities and Challenges by Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi Future Internet **2012**, 4, 621-645; doi:10.3390/fi4030621

[28] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, January 2013, pp. 131-143.

[29] M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.

[30] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.

[31] 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.