Volume 6, Issue 1, January 2019 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Communication of Secure Health Records in e-Health Cloud Through Attribute Based Encryption (ABE) Strategies

Mukta Bhatele
Professor
Department of Computer Science & Engineering
Gyan Ganga Institute of Technology and Sciences
Jabalpur, (M.P.) [INDIA]
Email: mukta_bhatele@rediffmail.com

Ayushi Chourasia
M.Tech. Research Scholar
Gyan Ganga Institute of Technology and Sciences
Jabalpur, (M.P.) [INDIA]
Email: achourasia127@gmail.com

ABSTRACT

Distributed computing is commonly a disseminated processing over a system. It assumes a vital job in human services combination costs, advancing assets in another time of advancements. Numerous medicinal services suppliers and insurance agencies today have received some type of electronic therapeutic record frameworks, the majority of the restorative records put away in incorporated databases as electronic records. Normally, a patient may have numerous social insurance suppliers, including essential consideration doctors, advisors, doctors and other restorative specialists. Patient may utilize numerous medicinal services insurance agencies for various sorts of protections, for example, therapeutic, dental, vision, etc. Sharing of individual restorative records is a patient driven model of wellbeing data trade which can be put away at outsider, for example, cloud suppliers. The classification of the individual wellbeing records is serious issue when persistent utilizations business online frameworks to store their wellbeing information, since it tends to be seen by everybody. Giving protection to their own restorative records is a promising strategy to encode the documents utilizing different cryptographic methodologies. There are different issues, for example, dangers for security of records, versatility in key administration and adaptable access have the most imperative difficulties towards accomplishing fine grained and cryptographically information get to control. To accomplish fine-grained and adaptable information get to control for PHRs, we utilizes attribute based encryption (ABE) strategies to scramble every patient's medicinal record document. This review depicts new methodology for secure capacity and controlled sharing of patient's wellbeing information

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

I. INTRODUCTION

The expenses of human services administrations rise and social insurance experts are winding up hard to discover the data then medicinal services associations are worried about wellbeing data innovation (HIT) frameworks. HIT enables wellbeing associations to give benefits in an all the more proficiently and cost-viably way. Innovations, for example, Cloud Computing (CC) give a solid foundation and offer HIT benefits over the Internet. This can be accomplished by a compensation as-you-utilize model of the "e-Health Cloud" to help the social insurance industry adapt to present and future requests yet downplaying their expenses. In the course of recent decades, PC frameworks are utilized broadly in medicinal and human services frameworks. For the documentation, stockpiling, handling, investigation and introduction of patient's data stockpiling gadgets and server frameworks are utilized in created nations today. Most human services frameworks are based on the premise that comprises of paper medicinal records, manually written test outcomes, digitized and non-digitized pictures, and transcribed notes. Sharing of data crosswise over suppliers is wasteful and uncertain and versatility of information is extremely uncommon. Every one of these procedures are tedious. Thus, there exist a lot more difficulties in this kind of frameworks where an expansive number of records are put away and information necessities are adaptable, adaptable, and simple to make, refresh, oversee and get to and so forth however security has highest need.

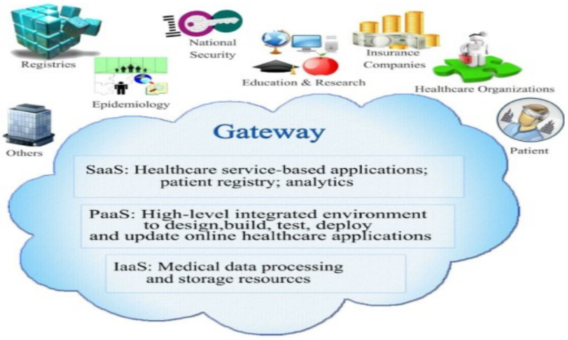
Registries
National Security
Education & Research
Insurance Companies
Epidemiology
Healthcare Organizations
Others
Gateway
Patient
SaaS: Healthcare service-based applications; patient registry; analytics
PaaS: High-level integrated environment to design,build, test, deploy and update online healthcare applications
IaaS: Medical data processing and storage resources

Figure 1: *Generic Architecture of e-health cloud*

e-Health Cloud as introduced in figure 1 is a Cloud that gives IT administrations to enhance patient's productivity. Regularly, the Cloud comprises of a variety of layered structure, beginning with the essential physical layer of capacity and server foundation and working up through the application and correspondence layers. The e-Health Cloud can be partitioned into various usage models dependent on whether it is made inside (private Cloud), redistributed (open Cloud) or a blend of the two (half and half Cloud).Cloud-based HIT arrangements utilized for patients, human services suppliers, and other concerned associations, for example, inquire about offices and insurance agencies and. The e-Health Cloud worried about a Gateway and Service-Based Applications. Passage: This part can be set to play out a few essential errands:

(i) overseeing access to the Cloud

(ii) confirming EHR (Electronic Health Record) given by various medicinal services suppliers as far as uprightness, realness, classification and security with restorative information trade

(iii) joining and incorporating EHR information into another Cloud-based EHR;

(iv) choosing and de-recognizing EHR to impart to the general population Cloud for research, instructive and mechanical purposes Administration Based Applications

For example, administrations for national security and the study of disease transmission, Web Portal, Picture Archiving, libraries and Communication Systems (PACS); all of which gave as administrations that are effectively overseen through CC operational parameters. Programming as a Service gives Cloud-based programming arrangements (e.g., clinical frameworks i.e.CSM) where customers, for example, medicinal services suppliers or money related and protection agents get access to the product capacities of the cloud. Stage as a Service broadens the essential framework with High-level coordinated condition to configuration, construct, test, convey and refresh online medicinal services applications. Framework as a Service manages the physical handling and capacity assets. Different components have been produced to protect and enhance security of the e-Health frameworks in the distributed computing. We introduces an outline of the protection safeguarding cloud wellbeing record framework utilizing characteristic based encryption approach that have been utilized in the e-Health mists. A Personal Health Record (PHR) benefit enables a patient to make, oversee, and control her own wellbeing related information in one place through the web, which makes stockpiling, recovery, and sharing of the therapeutic data in proficient way. Particularly, every patient is having the full control of her therapeutic records and can impart their wellbeing information to a wide scope of clients, including social insurance doctors, relatives or companions. Because of the staggering expense of building and keeping up specific and prepared server farms, the greater part of the PHR administrations are given by outsider specialist co-ops, for instance, Microsoft Health Vault. The objective of patient-driven security is regularly in struggle with versatility in a PHR framework. The approved clients may either get to the PHR for individual use or expert employments. Models are dear loved ones part while the last can be medicinal specialists, drug specialists, and scientists, and so forth. We allude the two criteria's of clients as close to home and expert clients, separately. Every proprietor is in charge of dealing with all the accessible expert clients by the key administration. In Existing framework a PHR framework demonstrate, there are various proprietors who may scramble as indicated by their own particular manners, conceivably utilizing distinctive arrangements of cryptographic keys. Each client acquires keys from every proprietor whose PHR she needs to peruse would restrain the openness since patients are not constantly on the web. Whatever remains of the paper is composed as pursues. Area II examines the Technical and non-specialized difficulties confronting e-Health Cloud. Segment III presents idea of Attribute based Encryption Technique. Diagram of the security saving methodologies utilized in the cloud based wellbeing record frameworks for example PHR are displayed in Section IV and Section V finishes up the talk and features the open research issues and regions.

II. Related Work

A few works has been endeavored to execute the idea of PHR upkeep framework. Ming Li Shucheng Yu, Yao Zheng, displayed approach of the protected sharing just as Revocable Attribute Based Encryption and adaptability of the clients and clarifies how open key cryptography utilized with the ABE just as Fine Grained Access Control. Y.Zheng examines the ace proposal for the saving the security of general wellbeing records in distributed computing and gives the great justifiable thought regarding the protection of the wellbeing records to keep up in the cloud. Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi featured chances and difficulties of e-wellbeing Cloud. S. Yu, C. Wang, and W. Lou, gives the information sharing dependent on characteristic and disavowal dependent on attributes. Ibraimi et al., has proposed anchored technique on PHR by applying attribute based Encryption, as it gives a protected Methodology. This technique does not depend on a focal specialist to give the way to the social or expert clients. This technique gives get to rights to the proprietor of the PHR. CP-ABE plot is utilized in this framework. S. Narayan, M. Gagne', and R. Safavi-Naini, gives the saving the protection of the Electronic Health Records framework with the utilization of the Attribute Based Infrastructure. Liang et al. proposed a self-controllable access strategy for the patients with the goal that they can have effectively access to their PHI (Personal Health Information). In any case, this occasionally causes the entire framework unbound. Sun et al. considered Privacy-saving wellbeing information stockpiling, where patients scramble their own wellbeing information and store it on an outsider server. Yu et al very much characterized access structure strategy dependent on KP-ABE for overseeing and putting away information in the cloud. Protection and classification of patient's data and utilization of mystery key for getting to information from the cloud are ensured in this sort of framework. Plus, a significant number of research works have demonstrated that utilization of fracture after encryption on information makes the information increasingly dependable and enhances the framework's general execution as potential gatecrashers dependably. Creator introduced the amazing method for getting to the information for example Fine Grained Access Control with the Multi Owners for getting to the records and gives the versatility to the clients for getting to the records.

III. Challenges of E -Health Cloud

1. Technical Challenges

a. Interoperability

The issue of interoperability is likewise confronted when incorporated e-Health Cloud administrations are given from both nearby and outside mists. One methodology is to utilize the idea of Service-Oriented Architecture (SOA) for executing the e-Health Cloud.

b. Availability

Most medicinal services suppliers require high accessibility of the e-Health Cloud administrations. Administration and information accessibility is vital for social insurance suppliers who can't adequately work except if their applications and patients' information are accessible. The e-Health Cloud administrations ought to be accessible consistently without any interferences or execution corruption

c. Scalability

Numerous medicinal services suppliers with a great many patient records could be taken care of by an e-Health Cloud, which is just feasible if and just if the administrations gave are adaptable. Cloud adaptability is basically empowered by expanding the limit and number of IT assets, for example, figure hubs, organize associations, and capacity units and giving appropriate operational and the board offices.

d. Data/Service Reliability

All e-Health Cloud administrations and information must be without blunder. Some critical choices with respect to single human or society wellbeing can be taken relying upon the information and administrations given by the e-Health Cloud. All things considered administrations are disseminated and may originate from various Cloud suppliers, the possibility of having defective or erroneous information or administrations can increment.

e. Flexibility

An e-Health Cloud must be fit for serving numerous human services supplier with various necessities. These necessities are as far as capacities, activities, clients, evaluating, the executives, and nature of administration (QoS) prerequisites. The e-Health Cloud ought to be truly adaptable in adding new required administrations to help medicinal services forms.

f. Data Management

Tremendous quantities of therapeutic records and pictures identified with a large number of individuals will be put away in e -Health Clouds. The information might be rehashed for high unwavering quality and better access at various areas and crosswise over extensive geographic separations. Most medicinal applications require secure, effective, solid, and adaptable access to the average records. These prerequisites authorize the need some stockpiling administrations that give adaptation to internal failure, secure capacity over open mists, and rich inquiry dialects that enable effective and versatile offices to recover and process the application information.

g. Security:

High security concerns are generally connected with open situations which are given by various specialist organizations and shared among various administration customers.. That is fundamental since information must be kept secure in the mists where it is put away alongside other human services suppliers' information.

h. Privacy:

protection is an imperative issue that could keep the full use of its abilities for various sorts of associations and applications. The worries include the capacity to shield patient's records from one another, other social insurance suppliers and the cloud specialist co-ops

2. Non-Technical Challenges

a. Organizational change

E-Health Cloud will require noteworthy changes to clinical and business procedures and furthermore to the hierarchical limits in the social insurance industry. Instances of such changes could be as new strategies, methods and work processes notwithstanding changes in how restorative procedures and documentation are finished.

b. Legislations and standards:

there are still no unmistakable or satisfactory enactments and rules for clinical, specialized and business practices of medicinal services in the e-setting. This incorporates the absence of models for restorative informatics, strategies, between operability, and transmission techniques in e-Health Cloud. As of now, there are a few gauges and characterizations for wellbeing data frameworks when all is said in done some of which can be received for the e-Health Cloud. One model is the International Classification of Diseases tenth modification issued by the World Health Organization (WHO). It characterizes a medicinal order list for the coding of ailments, signs or irregular discoveries, grumblings, social conditions, and outside reasons for damage or ailments. Another arrangement is The Systematized Nomenclature of Medicine (SNOMED) which was planned as a definite classification of clinical prescription to store as well as recovering records of clinical consideration in human and veterinary medication.

c. Ownership of Data:

Information possession in the business wellbeing all in all is a territory with no reasonable rules. This test is worried about the production of strategies and rules that draw clear proprietorship limits.

d. Usability and users experiences

This test is worried about the degree and dimension of appropriation gotten by the e-Health Cloud clients including patients, medicinal services experts, and regulatory and protection faculty. Legitimate and sufficient pre-usage preparing and showcasing alongside constant post-execution preparing are vital to help defeated this test.

E E-Health Cloud gives significant advantages to the medicinal services industry; it expands the real difficulties of HIT and CC together and adds more load to these difficulties as it is utilized to store and process delicate therapeutic information. Here we condense the specialized and non-specialized difficulties especially looked by the e-Heath Cloud.

4. Attribute Based Encryption Techniques -

At the beginning times of the distributed computing and individual wellbeing record the customary encryption methods were connected to the individual wellbeing record and now days the propelled encryption strategies with the end goal that quality based encryption and its distinctive varieties are utilized.

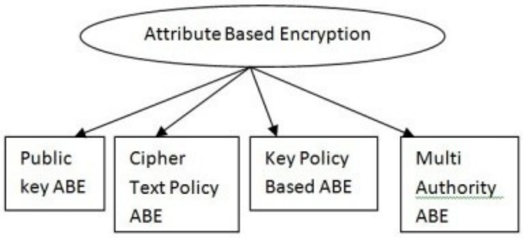

Figure 2: *ABE Techniques*

4.1 Attribute Based Encryption

Quality based encryption (ABE), one of most ideal personality based cryptographic frameworks where properties are taken as information and cryptographic activities are done on those attributes dependent on characterized strategies. Utilizing ABE system we are giving security to the database. In this the delicate data is shared and put away in the cloud supplier; it is expected to scramble figure content which is ordered by set of properties. A. Sahai and B. Waters give the instatement of Attribute Based Encryption just as point by point about the Fuzzy Identity Based Encryption procedures. In this framework both the figure content and mystery key will be related with the characteristics. The client who is having a base number of characteristics just can decode the information.

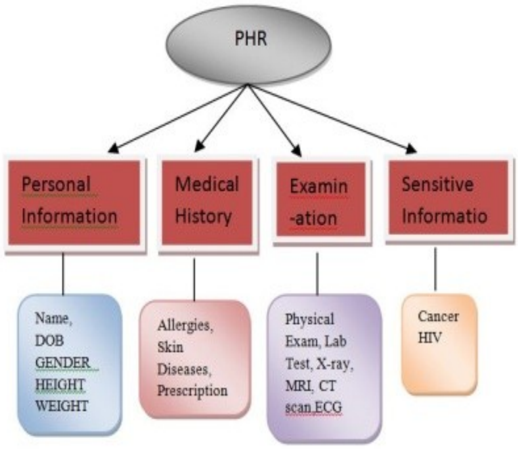
PHR
Personal Information
Medical History
Examin -ation
Sensitive Informatio
Name, DOB GENDER HEIGHT WEIGHT
Allergies, Skin Diseases, Prescription
Physical Exam, Lab Test, X-ray, MRI, CT scan,ECG
Cancer HIV

Figure 3: *Attribute Hierarchy of health records*

Open key encryption was the most customary strategy connected to the PHR for the security of the information. Be that as it may, it made the high key-administration issues and furthermore this strategy was less adaptable. Figure content Policy Attribute based Encryption (CP-ABE): procedure is utilized to keep encoded information classified The key-thought of the CP-ABE is: the client mystery key is related with a lot of attributes and each figure content will installed with an entrance structure.

The client can unscramble the message just if the client's quality happy with the entrance structure of the figure content. Key -Policy Attribute-based Encryption (KP-ABE) is a crypto framework for fine grained sharing of encoded information. In KP-ABE figure content are name with qualities and private key are related with access structures that control which figure message a client can unscramble. It is utilized for anchoring delicate data put away by outsiders on the web. The KP-ABE is valuable for giving the fine-grained get to control to the information framework where it can productively determine what part of information framework can be gotten to by which client and what are the tasks they can execute over yonder. Multi-Authority Attribute-Based Encryption (MA-ABE) is a propelled attribute based encryption in which it worried about numerous quality specialist for dealing with the distinctive arrangement of clients from various spaces. In the PHR framework the clients will be from various area like the specialists from human services associations, the loved ones from individual relations and different clients from protection space as well. Along these lines the MA-ABE plan will profoundly lessen the key-administration issues and it will give fine-grained get to control to the framework.

4.2 Proposed PHR System

Customary clinical settings worried about paper-based restorative records and remedies have likewise progressed to the Personal Health Records (PHRs) and the Electronic Health Records (EHRs).From the clinical perspective, it is essential to get to the exceptional incorporated patient wellbeing data. E-wellbeing cloud can be considered as a stage that, other than putting away immense volumes of the wellbeing information, additionally fills in as an organized administration of the wellbeing information over different social insurance suppliers. In the current framework the information proprietor is transferring the information to the cloud server, after encrypting the information as indicated by the entrance control approach characterized with the arrangement of qualities. This encoded information can be decoded by the client just if the properties of that client fulfills the entrance control arrangement. The issue tended to here is the privacy of PHRs. Patients records contains delicate data, for example, subtleties of a patient's illness, tranquilize use, sexual inclinations, and so on. Wrong revelation of a record can completely change patient, and there might be no real way to fix such damage fiscally or in fact. In this way, it needs insurance for patient's wellbeing records when they are transferred and put away in business Web-based frameworks. Think about after situation where a patient, has some touchy individual wellbeing records which she needs to store safely in a Web-based PHR, and offer them with different clients who have a place with two distinctive security areas: (1) proficient space (PD) - a human services supplier gathering, for example, specialists, medical caretakers, or (2) social space (SD) - her family, companions, or patients.

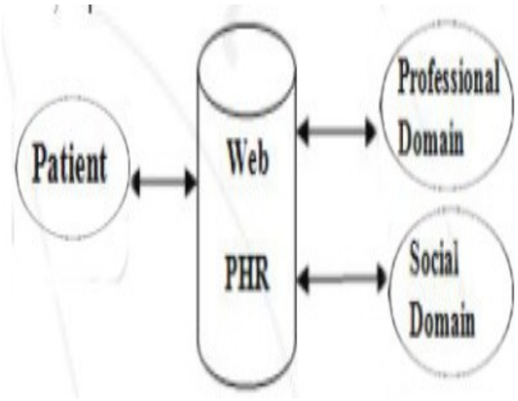

Figure 4: *Proposed PHR System Architecture*

The situation gives the thought regarding the requirement for a framework which satisfies the accompanying security prerequisites:

(a) Shield wellbeing records from system assailant. Along these lines, information is to be encoded before it is sent to the web PHR.

(b) Wellbeing records shielded from outsiders who store PHRs. The outsider oversees web PHRs which are not available to the plain information.

(c) The entrance strategy worried about the scrambled information, to such an extent that just those clients having a mystery key related with set of properties which fulfills the arrangement may be fit for unscrambling it.

(d) Clients from the expert area and clients from the social space both should be appropriately validated and approved to get to the information.

Arrangement of the issue in the current framework is overwhelmed by the Personal wellbeing record is keep up in the incorporate server to keep up patient's close to home and analysis data. A high level of patient's protection is kept up at the same time with the assistance of multi-specialist ABE. Proposed framework empowers dynamic change of access strategies or record attributes, bolsters effective on-request client/quality denial an under crisis situations. Expository and test results are exhibited which demonstrate the security, versatility and effectiveness and protection of our proposed plan. Use case graph of proposed framework is appeared in the fig:

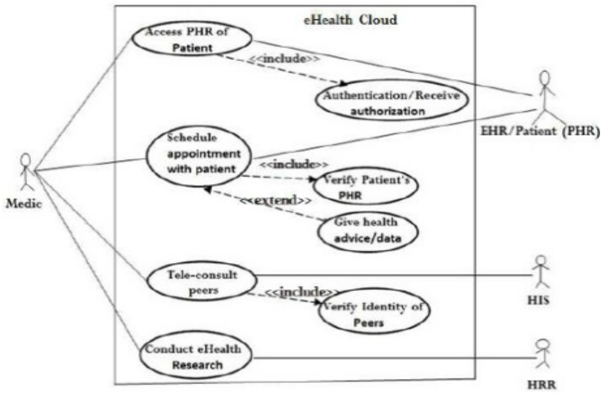

Figure 5: *Use Case flow of PHR System*

To accomplish fine-grained and adaptable information get to control for PHRs, we received property based encryption (ABE) strategies to scramble every patient's wellbeing record document We concentrated on different information proprietor situation, and gap the clients in the PHR framework into various security areas that incredibly decreases the key administration multifaceted nature for proprietors and clients with the assistance of MA-ABE procedure. In this framework, we satisfy the referenced holes by proposing a security structure display for patient-driven sharing of PHRs in a multi-space, multi-specialist PHR framework with numerous clients.

V. Conclusion

In this paper, we have proposed protection saving and secure sharing patient driven structure for keeping up close to home wellbeing records in distributed computing. With the assistance of somewhat utilized cloud servers, patients will full control through encoding their PHR records to permit fine grained access. This system worried about the extraordinary difficulties by various PHR proprietors and clients, in that we extraordinarily decrease the time, security and multifaceted nature of key administration. We utilized ABE strategy to encode the PHR information, with the goal that patients can permit access as the private clients, yet not open by people in general clients.

Acknowledgement

My true because of Dr. Mukta Bhatele madam for her accommodating conclusion and proposal for the paper.

REFERENCES:

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

[2] 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.

[3] 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.

[4] 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.

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

[6] 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).

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

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

[9] 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.

[10] 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

[11] 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.

[12] 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).

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

[14] 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.

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

[16] L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal

Health Records by Applying Attribute -Based Encryption," technical report, Univ. of Twente, 2009.

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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

[25] 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).

[26] 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.

[27] 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.

[28] 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.

[29] Varia, J. Cloud Architectures.

Available online: http:// aws.amazon.com/articles/ 1632 encoding UTF8 & jiveRedirect 1 (accessed on 28 June 2012).

[30] 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

[31] 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.

* * * * *