Middle-East Journal of Scientific Research 25 (6): 1326-1332, 2017
ISSN 1990-9233
© IDOSI Publications, 2017
DOI: 10.5829/idosi.mejsr.2017.1326.1332

Secured Medical Data Storage over Cloud for Comprehensive Treatment

Sathya Sankaran and Rajkumar Rajasekaran

SCOPE,Vellore Institute of Technology, India

Abstract: E-health is becoming an ideal, alternative approach to the traditional approach of handling and giving health care. This paper offers a solution for good health by observing and recording the details of each and every consultation made for a patient and not merely the storage of milestone observations. Every hospital, doctor and patient is uniquely identified, each patient is free to get treatment at any hospital, under any doctor, of their choice. Recording the observations made during every consultation helps in a better understanding of the patient's condition and results in a more comprehensive treatment. To maintain confidentiality, data is transferred from one place to another by encrypting and decrypting. An algorithm, Frequency and Difference algorithm is provided to provide security to text transferred from source to destination. This protects the data on its transit from one location to another. The hospital, doctor and patient are treated as objects involved in the system. The cloud offers a natural platform for providing health care, by virtue of the various services offered. The cloud provides a virtualized source of resources including hardware and software.

Key words: Cloud computing · Patient health record · Security · Frequency and difference algorithm

INTRODUCTION

The cloud offers various solutions for the general health and well being of patients. Patients are clinically observed and are prescribed treatments depending on the observations and results of various tests ranging from blood samples to scans. The doctor diagnoses the ailment depending on the results of the tests and observations made. A suitable treatment is administered to the patient. In this paper, we propose that we can store details of each and every consultation of the patient with a doctor and not restrict ourselves to particular consultations which are of apparent importance to the patient. Every consultation has its share of observations, sample tests, scan tests and so on and thus when the records of all consultations are stored; it helps in understanding the pattern of the ailments of the patient. A better and more comprehensive treatment is possible. Take for instance the case of a diabetic patient whose sugar level is not normal. Readings taken of the patient's blood glucose level over a continuous period, helps in administering the suitable dosage of medicine, ensuring stable blood glucose level and thus good health. This is in contrast to the condition of the patient who is not monitored on a regular basis. An encryption decryption algorithm Frequency and Difference is proposed.

Literature Review: This study is to find how user friendly the systems using personal health records are to the adults with low literacy level and who are not economically empowered [1]. Systems using various types of personal health records including that which are associated with Electronic health records are used. The users find the features useful such as, requesting appointment, requesting further prescription etc. Three systems, System A, System B and System C were studied. They all have user interface that is menu driven and separate menus for some complaints such as diabetes and so on. System C made statements such as 'Quit smoking'. A list of tasks was identified for testing. Each of System A, System B and System C complied with some of the tasks and did not have one or two tasks. The tasks were like finding the test reports, arranging an appointment with the doctor and so on. Completion of tasks with participants revealed that health and text literacy is required to work with these systems. A sample study was done with 54 participants from the age 22 to 62.It included a major population that worked with computers for various reasons. An observer marked the user's response to the options on the screen. A mathematical modelling of the scores obtained by summing the scores for choice in the PHR is done. Navigating through the screens to find the appointment fixing screen is a difficulty.

Corresponding Author: Sathya Sankaran, SCOPE, Vellore Institute of Technology, India.

There is such kind of difficulties, including cognitive capabilities. Finally, it is understood that there should be a user centric approach for designing the PHR.

E-health records are like e-tickets storing medical data of a person [2]. It is an alternative to bulky paper files and provides ease of updating and sharing. The concept of EHR is taking shape in the U.S.A and the U.K. Australia is implementing EHR for all its citizens. EHR has data such as department, test results, diagnosis, treatment and other such information. The architecture of the proposed model is divided into four tiers. Tier 1 connects to the internet the centralized EHR. In tier3, the community health centres are interconnected to the primary health centres. Tier1 provides EHR for every citizen. Patient monitoring system, Public health centralized health record is available in the tier1.Big data analytics is used to handle the large data set. Data mining algorithms are used on them. Feature extraction is done using Rtool which is used for simulation.

Personal Health Records are used to store patients' health information [3]. Depending on the symptoms the patients are suggested diseases which are likelihood to occur, so that patients take essential steps. Cloud servers are used to store patient health records. Confidentiality is provided by encrypting the message and applying an erasure code. Attribute based encryption is adopted. Third party storage is used and information is accessed through queries. One has to take care of reliability and security on cloud storage. Security is achieved using proxy re-encryption method. Patient information is encrypted before it comes to the cloud server. A key authorizes an actor to view the required information. A new key is required for every viewing. People accessing sensitive data, like doctors should be given an authorized key from the cloud server. On applying the key, the actor can see the required data. Actors that request access to sensitive data need to be authorized with a key.

This paper focuses on Personal Health Records from the aspect of activation [4]. Activation is the ability of the person to take care of oneself independently by moving to take their medication etc. This is important for older adults. This paper is a study of the lack of diversity with senior adults when it comes to using personal health records. Out of thousands of abstracts, ten publications met the inclusion criteria. Demographic study was done in the use of personal health records. Gender was another criterion where the participation of the female gender was lesser than the counterpart. It was concluded that senior adults who were convinced with the personal health record method were ready to accept it. However there is still lack of diversity in the study as not many countries have tried the personal health record method of medical practice.

This study performs visualization of electronic health record data from late 1990s to 2013 [5]. Investigation was done on the documents using MEDLINE and Web of Knowledge. The final analysis included 18 articles by filtering from eight hundred and ninety one articles. Initially, visualization was done for single patient with complex data. Later, investigation was done for a huge number of patients. As the electronic patient records are colossal in number, it can be useful for knowledge discovery if the data is organized well. The issues in visualization will help in designing visualization techniques with improvements.

The E-health cloud system has sensitive data, which must be protected [6]. Initially the PKI infrastructure was used by many which are burdensome as each user had to remember their public and private keys. Identity based encryption uses its identity as the public key. In this paper we proposed many identity based schemes such as new IBE schemes and new IBPRE (identity based proxy re-encryption) schemes. Their security is proved.

Electronic Health Services (EHS) provide healthcare at a lower cost and with efficient means [7]. However, there are security, privacy and integrity concerns. This paper is a survey of the above concerns in EHS that is method based. Architecture is an important factor and it may be distributed or cloud based. Access control may be role based, attribute based or identity based. Sharing of data among hospitals and health care providers is another important factor.

The necessity to put data in a cloud or not depends on the security required by the data that is stored [8]. This paper provides a complete study of the principal threats that hinder cloud computing to be taken up on a large scale. This paper gives an idea of the directions of the upcoming security schemes. A selection of the best of propriety and Open Source cloud offerings is made and a study is done on this. This paper can be used as a tool to gain insight into cloud security and also to understand the merits and demerits of the cloud solutions.

Cloud computing makes is possible to meet various requirements on Web-based service offerings [9]. But the cloud contains sensitive data which must be protected by ensuring cloud security and privacy. This aspect makes the users worry. Also, it leads to hindrance in applying the cloud concept in the financial sector and the government sector. This paper proposes a clever cryptographic approach by which the cloud user can directly get access to partial data.

Wireless Body Area Networks are useful in health [10]. They felicitate cloud computing and communication. But they are subject to security issues. This paper proposes a network with four layers: perception, network, cloud computing and application. Possibility to work with WiFi and LTE for this network is made possible by integrating TCP/IP and Zigbee in the four layered network.

A detailed state of art on the various service models in cloud SAAS, PAAS, IAAS and the corresponding security issues in each service model and the existing security solution are also discussed [11]. The solution would give 'Security as a Service' to the applications by giving security as a solitary level or a multi-level in light of the application's prerequisite also, expansion to it, the levels are empowered to change progressively making the security framework less unpredictable.

The cloud offers various advantages such as a large storage, lower cost etc., but one of the challenges that does not allow companies to take to the cloud, is the lack of complete and strong security [12]. This paper provides a combination of methods to provide security to the owner to the user. The methods are divided into two phases, Phase I and Phase II. Phase I deals with techniques for secure the data from the start up to the storage of it on the cloud. Phase II provides protection during the retrieval of data.

In earlier times, electronic health records were stored in an exclusive system [13]. They had their own dedicated servers and networks to cater to their hospital needs. The aim of this work CloudHealth has been to create a common platform on the cloud for hosting the records and services of an entire country. Requirements like 100% uptime, accessibility across the globe, maintaining security are offered as Software as a Service. CloudHealth has been designed with two parts namely Infrastructure and Services.

This work deals with sharing information relating to health, which is a must for progress in e-health [14]. The above is achieved using cloud computing and a Google App Engine. The cloud offers a suitable channel to facilitate a quick access to patient health information which helps in quicker treatment. Privacy and ownership issues determine e-health on cloud computing.

Cloud offers tremendous opportunity in health care information science research and information sharing [15]. But it also has certain limitations such network security, privacy etc. The paper discusses the challenges in health information sharing being applied in health cloud and comes up with approaches to conquer those challenges. A new presentation of cloud is introduced, as a stack model, of storage, computing, virtual resource layer and external application programming interface.

In places like China, health care is concentrated on cities and rural areas lack the required health care [16]. In this research HCloud platform has been developed for health care. As a first step, through wired or wireless means physiological signals are received from the patients and sent to the cloud. Next, using data mining technology, the data collected is analyzed in the cloud. As the last step, the results are given as feedback and suggestions are given to the user.

Cloud Computing: The cloud is a virtualized distributed and parallel computer network that acts as a provider of resources such as hardware, storage, network, applications, services etc. It is considered as a pay-per-use model for providing resources to the user. The cloud is scalable and appears to be a source of infinite resources. Computing is delivered as a utility. This utility is offered over Internet as Web services. Applications like Google and Facebook are on the cloud.

Different operating systems, each with a set of software, can run on a single physical platform. This is Hardware Virtualization and is facilitated by software called hypervisor or Virtual Machine Monitor.

The classes of cloud computing services are a. Infrastructure as a Service b. Platform as a Service c. Software as a Service. Infrastructure as a Service offers virtual resources. Considering the Platform as a Service domain, an environment to develop and host applications is available. Considering the Software as a Service domain, it is possible to build applications from a group of component services. For example e-mail can be used again as a part of a business solution. The resources are abstracted. There is self-service interface.

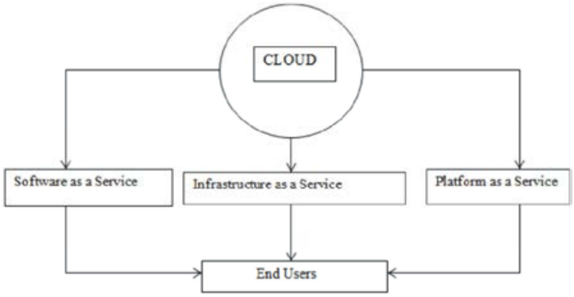


Fig. 1: Cloud Computing

This paper recommends the proposed work to be considered in the cloud computing paradigm for the technology offered by cloud computing and its advantages. The storage of data related to each and every consultation is feasible as the cloud offers virtually an infinite space. The encryption and decryption algorithms suggested suit the application proposed.

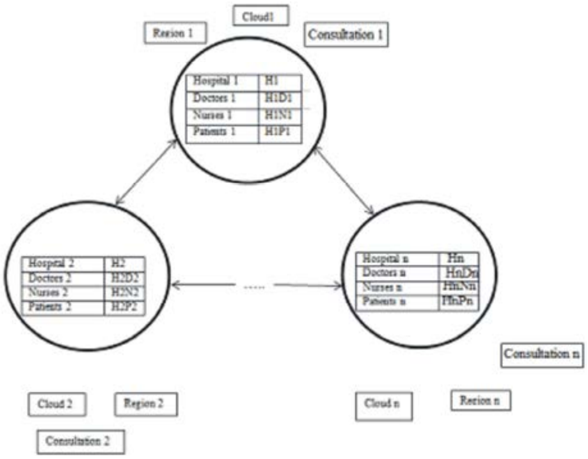
Proposed Methodology: The scenario under consideration is the presence of information about hospitals offering treatment for various complaints, on the cloud. Each hospital has doctors in various departments. The doctors treat the patients depending on the complaints. This information is also available on the cloud. The architecture diagram depicts that any patient is free to move to any hospital and avail the treatment given by the doctors there. They are also free to avail the services rendered by the nurses in any hospital. Fig. 2.0 explains the same.

The diagram Fig. 3.0 shows hospitals interconnected to one another. Thus, a patient receiving treatment from one doctor in one hospital is free to shift to any other hospital.

Hospital Record: Every hospital is represented by an object. The attributes representing a hospital are Hospital id- a unique number identifying a hospital, the name of the hospital and its address as depicted in Table.1.1. This again is unique as any address will be unique.

Table 1.1: Hospital Record

Hospital id	Hospital Name	Hospital Address



X-integer HX – Hospital id DX-Doctor id NX-Nurses id PX-Patient id

Fig. 2.0: Consultations made and collected at various clouds located in various regions

Doctor Record: Every hospital has doctors. Each doctor is considered as a unique object. It is represented by a unique doctor id along with hospital id of the hospital for which the doctor works the doctor's name and his field of specialisation. This is depicted in Table.1.2.

Table 1.2: Doctor Record

Doctor id	Hospital id	Doctor Name	Specialisation

The hospitals have patients. Each patient has a unique patient id. It has records for each consultation. Each consultation contains data regarding the hospital, the doctor treating the patient, information related to the tests undertaken, the diagnosis and treatment offered. The patient's record is illustrated in Table 1.3. As seen, the patient record is meant for each consultation which also stores information regarding the hospital at which the treatment was undertaken, the doctor consulted, the nurses who were involved, the symptoms, vital signs, reports, other observations, diagnoses made as well as the treatment offered. A patient is free to receive treatment from any doctor in any hospital. Note that the data stored for a consultation is only suggestive and not thorough.

Figure 3. depicts the condition, wherein each patient is receiving treatment from any doctor belonging to any hospital. PATIENT ID1 can receive treatment from any doctor listed as D1 1, D1 2,.. D1 K from HOSPITAL ID1 or from any doctor listed as D2 1, D2 2,.. D2 M from HOSPITAL ID 2 and so on up to any doctor listed as DN 1, DN 2,.. DN R from HOSPITAL IDN. The same holds good for all patients.

With the concept of Big Data taking up the world, there is no dearth of storage space for storing the patients' information as depicted. Storing information about each consultation enables a continuous monitoring of the patient. This helps in a better diagnosis. It also keeps track of the progress of the patient and helps in better treatment. It also helps in a quicker and a better recovery.

Consultations may be from the same hospital and consecutive consultations may be recorded for each patient in the same hospital as in the format given, where the Hospital from which treatment is availed is indicated as Hospital X.

Table 1.3: Consultation Records of a Patient

Patient Records	Patient id							
Consultation 1								
Hospital id 1	Doctor id 1	Nurses id 1	Symptoms	Vital Signs	Reports	Other observations	Diagnosis	Treatment
Consultation 2								
Hospital id 2	Doctor id 2	Nurses id 2	Symptoms	Vital Signs	Reports	Other observations	Diagnosis	Treatment:
Consultation n								
Hospital idn	Doctor id n	Nurses id n	Symptoms	Vital Signs	Reports	Other observations	Diagnosis	Treatment

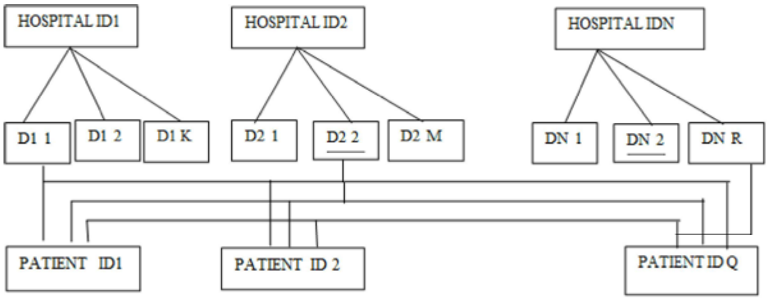


Fig. 3: Patient consults different doctors at different hospitals

HOSPITAL ID1 –identifier of hospital 1
HOSPITAL ID2 – identifier of hospital 2
HOSPITAL IDN – identifier of hospital N
D1 1 – identifier of doctor 1 working in hospital 1
D1 2 – identifier of doctor 2 working in hospital 1
D1 K – identifier of last doctor working in hospital 1
D2 1 – identifier of doctor 1 working in hospital 2
D2 2 – identifier of doctor 2 working in hospital 2
D2 M – identifier of last doctor working in hospital 2
DN 1 – identifier of first doctor working in hospital N
DN 2 – identifier of second doctor working in hospital N
DN R – identifier of last doctor working in hospital N
PATIENT ID1 – identifier of first patient receiving treatment from doctor 1 in hospital 1, doctor 2 in hospital 2, doctor R in hospital N
PATIENT ID Q – identifier of third patient receiving treatment from doctor 1 in hospital 1, doctor 2 in hospital 2, doctor R in hospital N

Frequency and Difference for Encryption/Decryption: The frequency algorithm works on text data that is to be transferred from one place to another. Any text data, reflects the frequency characteristics of a language. For example in English, 'e' is one of the most frequent letters and 'z' is one of the least frequent letters. To send a text without revealing itself, this frequency of the language must be changed. Here, we remove the letters with high frequency and store their positions. Then, we convert the text such that all letters have the same frequency. Then we subtract letters at equidistant positions starting from the first position. This subtraction is done on the result of the previous stage starting from the first position. This is repeated for some number of iterations. Then the result is sent to the destination. At the destination, a reversal of each operation done at the source is done.

Encryption:

- Remove letters with high frequency such as 'E', 'T', 'A' from the text and store their positions.
- Find the next letter with highest frequency and the letter with lowest frequency. Add their count and get the average value.
- Reduce letters with frequency higher than the average to the average frequency by removing letters at random positions and storing their positions.

- Increase letters with frequency lesser than the average to the average frequency by adding letters at random positions and storing their positions.
- Map the letters to numbers ranging from thousands to one, with a repeating sequence of ten thousands, thousands, hundreds, tens and digits.
- For example V-50000, W-3000, X-400, Y-89, Z-2
- Find difference of 1st and 101st character, 2nd and 102 nd character and 101st with 201st 102nd with 202nd so on.
- Repeat difference as above for a few iterations on the sequence resulting from the previous step.
- Record the 1st character value of each iteration.
- Only the resultant difference value is sent over the network to the destination.

Decryption:

- The first character of each iteration is added to next value in the difference algorithm, for example 1st value with 101st value ; 101st value with 201st and so on.
- This is repeated for the same number of iterations for which difference was found.
- Replace the mapped values with the letters.
- Remove the low frequency letters that were added using the stored positions.
- Add the high frequency letters that were removed using the stored positions.
- Add the removed letters such as ‘E’,’T’,’A’ at their original positions.

Frequency Analysis Comparison: The following is the comparison of frequency analysis on various algorithms.

Table 2: Frequency Analysis Comparision

Aglorithm	Frequency Analysis
DES	Vulnerable to frequency analysis
AES	Immune to frequency analysis
Blowfish	Immune to frequency analysis
Frequency and Difference Algorithm	Immune to frequency analysis

CONCLUSION

This paper has emphasized the advantages of storing and using all consultations of a patient. However, in further research, it may be possible to identify patterns of illness, disorders etc. and work out periodic consultations and storage of such periodic data instead of all consultations. The ultimate aim is to improve the health conditions of the patients. The Frequency Difference Encryption algorithm will work for any language by removing the pattern aspect of the language.

REFERENCES

1. Czaja, S.J., C. Zarcadoolas, W.L. Vaughon, C.C. Lee, M.L. Rockoff and J. Levy, 2015. The usability of electronic personal health record systems for an underserved adult population. Human Factors: The Journal of the Human Factors and Ergonomics Society, 57(3): 491-506.
2. Kavitha, R., E. Kannan and S. Kotteswaran, 2016. Implementation of cloud based Electronic Health Record (EHR) for Indian healthcare needs. Indian Journal of Science and Technology, 9(3).
3. Dhivya, P., S. Roobini and A. Sindhuja, 2015. Symptoms based treatment based on personal health record using cloud computing. Procedia Computer Science, 47: 22-29.
4. Kneale, L. and G. Demiris, 2017. Lack of diversity in personal health record evaluations with older adult participants: a systematic review of literature. Journal of Innovation in Health Informatics, 23(4): 789-798.
5. West, V.L., D. Borland and W.E. Hammond, 2015. Innovative information visualization of electronic health record data: a systematic review. Journal of the American Medical Informatics Association, 22(2): 330-339.
6. Wang, X.A., J. Ma, F. Xhafa, M. Zhang and X. Luo, 2017. Cost-effective secure E-health cloud system using identity based cryptographic techniques. Future Generation Computer Systems, 67: 242-254.
7. Yüksel, B., A. Küpçü and Ö. Özkasap, 2017. Research issues for privacy and security of electronic health services. Future Generation Computer Systems, 68: 1-13.
8. Coppolino, L., S. D’Antonio, G. Mazzeo and L. Romano, 2016. Cloud security: Emerging threats and current solutions. Computers and Electrical Engineering.
9. Li, Y., K. Gai, L. Qiu, M. Qiu and H. Zhao, 2016. Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences.
10. Hassan, M.M., K. Lin, X. Yue and J. Wan, 2017. A multimedia healthcare data sharing approach through cloud-based body area network. Future Generation Computer Systems, 66: 48-58.
11. Subashini, S. and V. Kavitha. 2011. A survey on security issues in service delivery models of Cloud computing. Journal of network and computer applications, 34(1): 1-11.

12. Sood, S.K., 2012. A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6): 1831-1838.
13. Hendrick, E., B. Schooley and C. Gao, 2013, January. CloudHealth: developing a reliable cloud platform for healthcare applications. In Consumer Communications and Networking Conference (CCNC), 2013 IEEE pp: 887-891.
14. Hu, Y., F. Lu, I. Khan and G. Bai, 2012, December. A cloud computing solution for sharing healthcare information. In Internet Technology And Secured Transactions, 2012 International Conference for IEEE. pp: 465-470.
15. Guo, Y., M.H. Kuo and T. Sahama, 2012, December. Cloud computing for healthcare research information sharing. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on IEEE. pp: 889-894.
16. Fan, X., C. He, Y. Cai and Y. Li, 2012. December. HCloud: A novel application-oriented cloud platform for preventive healthcare. In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on IEEE. pp: 705-710.