Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 135 (2018) 688–699

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Computer Science and Computational Intelligence 2018

Private cloud solution for Securing and Managing Patient Data in Rural Healthcare System

Raghavendra Ganiga, Radhika M Pai*, Manohara Pai M M, Rajesh Kumar Sinha[a]

Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, India

[a]*School of Allied Health Science, Manipal Academy of Higher Education, Manipal, India*

Abstract

Rural healthcare system in India is managing patient data in a traditional paper based system. Most of the rural hospitals in India are lacking in resources to maintain and manage the patient health data. As the world moves towards digitization, one of the key challenges in developing countries like India is in making the healthcare data accessible from rural to urban in digital form. Advancement in IT technology in healthcare sector has made it possible to maintain and manage the patient data in digital form in all levels of healthcare system. Cloud computing has emerged as a main in providing healthcare IT solution. Therefore, rural healthcare organizations should move towards building their own private cloud infrastructure which could be an excellent solution for the country's needs to have improved healthcare in rural areas. In private cloud, medical data is stored in databases in which some of the data in a medical database is sensitive in nature and access to this data should be limited to authorized persons. In this paper we propose a secure cloud architecture by building private cloud. The proposed private cloud architecture makes use of two database one for storing medical record and another for key. To reduce the risk of the health information leakage and safeguard the health data, hash and the encryption operation are performed before transmitting to the cloud database. With this technique, path for a third party to obtain the sensitive information stored in the cloud is being blocked. Therefore the proposed framework provides better secured services to the users.

Keywords: Rural; Healthcare; Private ;rural; cloud;encryption

* Corresponding author. Tel.: +91-994-567-1361
E-mail address: radhika.pai@manipal.edu

10.1016/j.procs.2018.08.217

1. Introduction

The world's population is growing rapidly[1]. Developed countries have been facing the trend of population aging, escalating costs, inconsistent provision of care, and a high burden of chronic diseases related to health behaviors. This situation makes healthcare management more and more important to all types of healthcare organizations. Health care is delivered mainly through Primary Healthcare Centre (PHC), Secondary Care Centre (SHC), and Tertiary Care Centre (THC)[2]. The different levels of healthcare system is depicted in Fig. 1. The primary healthcare centre deal with patients whose medical conditions can be managed on an outpatient basis. The secondary healthcare usually deals with acute care hospitals whereas tertiary care requires the resources of a sophisticated medical center.

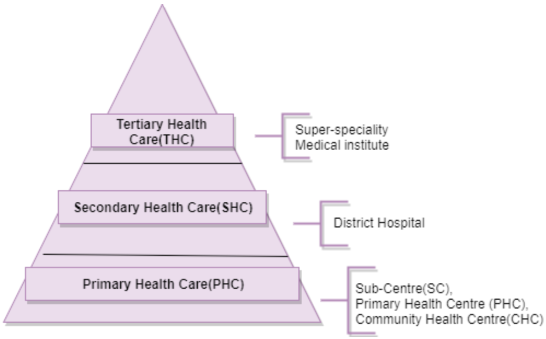

Tertiary Health Care(THC)
Super-speciality Medical institute
Secondary Health Care(SHC)
District Hospital
Primary Health Care(PHC)
Sub-Centre(SC),
Primary Health Centre (PHC),
Community Health Centre(CHC)

Fig. 1. Different Levels of health-care system

Healthcare ecosystem consists of physicians, nurse, pharmacist, radiologist, lab technician, and patient. Cloud computing helps in organizing the medical record at different levels of healthcare setting. Cloud computing is a promising and emerging technology for the users of the healthcare ecosystem[3] by connecting many health information management systems together with laboratory, pharmacy, radiology etc. The main obstacles and serious problem towards the rapid growth of cloud computing are data security and privacy issues. Most of the healthcare users of private cloud do not fully trust the inside threat of the healthcare organization for safeguarding sensitive health information[4] data because there is no governance about how this information can be used by them and whether the healthcare organization actually control their information.

As part of the field study, hospitals at different healthcare levels namely Primary Healthcare Centre (PHC), Secondary Care Centre (SHC), and Tertiary Care Centre (THC) in Udupi district, Karnataka were visited. Field study was conducted to understand the IT-infrastructure facility used for managing and maintaining the patient information. During this study it was observed that, in PHC levels, namely sub center, primary health center and community healthcare center are maintaining yearly paper-based records such as registration book, examination book and treatment book. In the record room only current five years of patient data is maintained and previous ones are discarded. Because of this the continuous health data about the patient is lost. Hence present requirement for Indian healthcare scenario is to capture lifelong summary of the patient from pre-birth to post-death with better IT infrastructure facility. Table 1 shows the present infrastructure facility in PHC levels.

Table 1. Infrastructure Facility in PHC levels

Levels and Facilty	Total computer facility	Router facility (Broadband)	Printer	Scanner
Sub Centre(SC)	0	0	0	0
Primary Health Centre(PHC)	1	1	1	1
Community Health Centre (CHC)	2	1	2	2

To implement IT infrastructure in rural[5] healthcare system, the main obstacle is requirement of the high speed INTERNET connectivity. To address this national level problem, the government of India has proposed a new project BharatNet for providing high-speed broadband optical connectivity to all rural areas. With this communication infrastructure all rural places in India will get 1 Gbps (Gigabyte per second) bandwidth capacity at rural level setting. Additionally,the government requested Telecommunications(Telecom)[6] company to list all unconnected villages in India and have planned to connect with Telecom services by 2020.

Internet connectivity with optical network improve the accessibility of health information within and outside the healthcare system. To build the health management system, the availability of the budget plays an important role. Many healthcare system prefer to move their IT infrastructures from being a capital expenditure (CAPEX) toward an operating expenditure (OPEX) model[7]. If healthcare organizations decide to maintain an internal data center such as CAPEX business model, there are the direct costs that accompany running a server: power, floor space, storage, and IT operations to manage those resources. There are also indirect costs of running a server, including the network and storage infrastructure and IT operations by the public infrastructure provider.

Rural healthcare needs to focus mainly on cost sensitive open source platform for deploying IT infrastructure in deferent levels of healthcare system[8]. To build an effective platform many open sources tools are available such as open stack, cloud stack and eucalyptus. In this paper, as a case study to manage patient data at rural healthcare setting by building a private cloud using open source tool is proposed. As far as infrastructure provisioning is considered for cloud, there are only two major players OpenStack and Eucalyptus. Infrastructure provisioning involves a provisioning tool to supply virtualized resources on-demand. Both Eucalyptus and Openstack are designed to be API-compatible[9] with Amazons EC2 platform.

The patient data which is stored in the cloud database is susceptible to attack on the current healthcare system. The data which is stored in the cloud should be protected from the attacker[10 11]. To deal with security, secure cloud model is built and tested with the proposed architecture model.

In this paper private cloud solution for managing patient data in rural healthcare system is proposed. Current version of private cloud model is deployed in community health centre and given access to all lower level healthcare system. According to digital India initiative, the rural healthcare system is going to improve with respect to INTERNET connectivity. Hence the system will be useful to connect all rural healthcare system.

The paper is organized as follows. Section 2 gives background study. In section 3 methodology about building private cloud in rural healthcare sector is discussed. Section 4 describes authentication and authorization model for open source cloud. Results are discussed in section 5. Finally, section 6 concludes the paper.

2. Background

According to Cloud Computing Survey[12] the private cloud was the most popular cloud deployment scheme of 2013. Although cloud computing has its advantages, it still has some issues to overcome. These issues include security of data, complete control over the cloud infrastructure, network latency issues and full access of the cloud environment.Many organizations prefer storing mission-critical data in their own infrastructure. Addition of dedicated components is possible when the cloud is owned by the organization. Wang et al[13]. discussed about how information technology can be adopted in the healthcare to automate the process flow from old technology. They also discussed about the use of service-oriented architecture (SOA) during implementation of web-based healthcare platform techniques, and also considers some of the implementation factor which requires active recommendation and customization in health care services.

Robert Birke et al[14], discussed about how corporate data centers uses virtualization as a mainstream technology in current scenario and explained about how virtualization allows efficient and safe resource sharing in data Center. Author additionally discussed about changes in VM patterns by configuring memory and process settings of the VM. David Freet et al[15], proposed effective cloud based computing services for cloud based applications. They used varieties of hypervisors such as XEN, KVM and ESX for cloud deployment model. They also analyzed the performance of hypervisor by allowing simultaneous execution of entire OS instances. Repu Daman et al[16]. proposed an architecture for health cloud infrastructure in terms of security models. They discussed about how to protect patient data in private public cloud environment and also discussed security mechanism namely role based access control , data encryption, digital signature and time to time security audits for healthcare data.

A good amount of research has been conducted in both cloud data access systems as well as storage system. Khan and Sakamura et.al[17] proposed a Discretionary Access Control (DAC) framework that provides healthcare organizations against security attacks and ascertains confidentiality of patient data. A trust-aware RBAC model has been used to demonstrate social healthcare networks application in a cloud environment[18]. A similar cryptographic RBAC model has also been designed that considers inheritance of the roles as well their hierarchy in the evaluation of trustworthiness of the users and how it can be deployed on the cloud[19]. Yu, Wang, Ren and Lu have combined Attribute-based encryption[20], proxy re-encryption and lazy re-encryption to achieve user access privilege confidentiality and secret key accountability of the users . An emergency medical system has also been developed to enable ubiquitous access to medical services[21]. Besides access control systems, efforts have also been to ensure that records have been stored after encryption and that data is transferred over a secure connection. Zhifeng Xiao et al.[22] identified five most important security and privacy attributes such as integrity, availability, confidentiality, accountability and privacy preserve. In addition , author described about administrative and technical safeguard. Using administrative safeguards unauthorized disclosure of patient data through inappropriate email are prevented. In technical safeguard, access controls mechanism is incorporated to prevent unauthorized access to patient information.

3. Methodology

This section discusses about manging the patient data by building a private cloud with proposed security mechanism.

3.1. Private cloud solution to manage patient data in rural healthcare system

Fig. 2 shows the architecture of proposed model which describes one simple application of IaaS on private cloud using EUCALYPTUS. For this purpose, Faststart model of installation was used with Eucalyptus version 3.4.2. All the necessary setup was done and an instance was launched with the custom Ubuntu Karmic (9.10) image. Then by accessing the instance from terminal using ssh, proper network settings like proxy settings, dns servers were configured and the internet connection was given to the instance. Using this connection, tomcat6 was installed on the instances of Ubuntu operating system. Although limiting the access of private cloud to intranet is vital as it provides

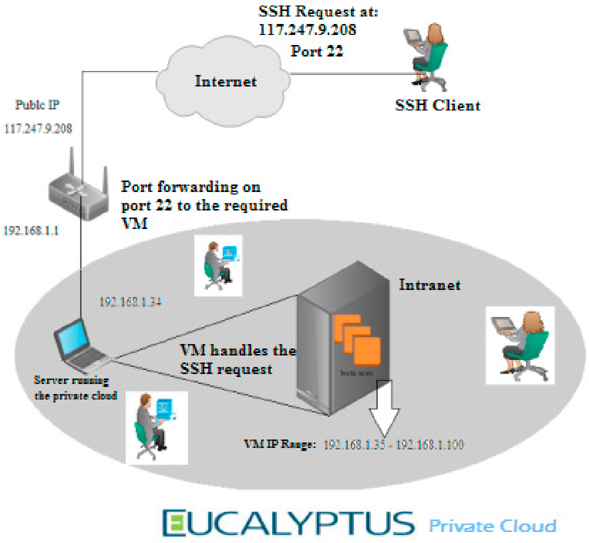


Fig. 2. Opensource methodology for managing patient data in rural healthcare system

security, it may be necessary to provide access to the private cloud from outside the intranet (Internet). Providing access means providing access to one or some of the VMs that are running on the private cloud. These VMs can be accessed using ssh which uses port 22. The basic idea is to use a public IP address and assign it to the VM to which the access is to be provided by using port forwarding for all ssh requests on port 22. This can be done on the router which is used to connect the server(s) running the private cloud to the INTERNET. Private cloud is mainly built for accessing the data from the intranet of the organization. The provision is given to the user to access the private data remotely using port forwarding techniques as shown in the Fig. 3. This concept was tested on the private cloud using a single public IP address. The server running the private cloud was connected to the INTERNET using a router. A VM was started on the cloud with a local intranet IP and the router which had the public address assigned to it was configured to forward all requests on port 22 to the VMs local IP address. Now from the INTERNET, an ssh request was sent to the public IP address.

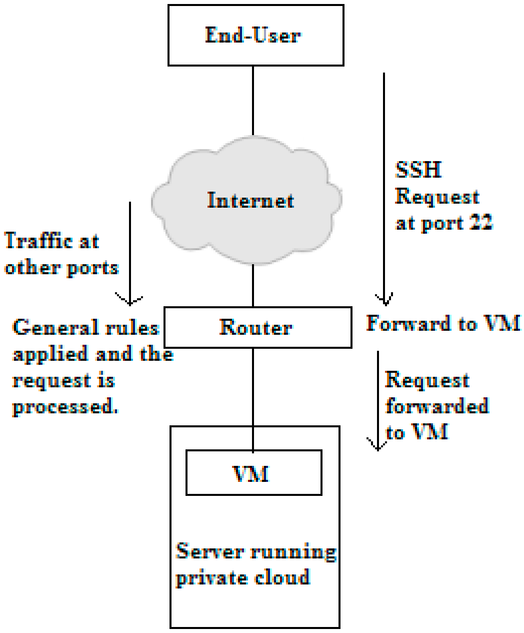


Fig. 3. Access the private data remotely using port forwarding techniques

The request first reaches the router on port 22 as it has the public IP address and not the actual VM. As the router is configured to forward all packets at port 22 to the VM, the request now reaches the VM which handles it and responds back to the IP address from which the request was generated. For providing access to multiple VMs, multiple public addresses can be used and the router has to be configured suitably. Apart from this, the private cloud was used to host a simple website as well by using port forwarding on port 80.

3.2. Supporting infrastructure for sustainability

The proposed private cloud model ensures or supports high availability as shown in the Fig. 4. The model is durable and likely to operate continuously without failure for a long time. Also fault tolerance characteristics features allows to remain in operation even if some of the component used to build the system fail. Major building blocks of high availability architectures are healthcare user, load balancer, availability zone, snapshot and replication layer.

The healthcare users are requesting health care services from the health information system and receiving response from the system. With load-balancer features, availability of the system increases by distributing the load between the zone. The request always move to the healthy running instances instead of going to the unavailability zone. It also automatically distributes the incoming application traffic among multiple instances using the load-balancing facility. Also load balancer is configured to handle encrypted (HTTPS) traffic, session persistence, health checking, and more.

The availability zone is another major component of the architecture where it is hosted in multiple locations. These locations are composed of regions and availability zones. Each region is a separate geographic area. Each region has multiple, isolated locations known as availability zones. It provides the ability to place resources, such as instances, and data in multiple locations. Snapshot feature provides the backup of the instances during the instance failure. The backup layer protect from failure. The health information data is stored in global database. Health care users are allowed to perform read, write and update the health data which is stored in the primary database. The data replication layer provides the functionality of switching data between primary and secondary database. In case if primary fails still user can access data from the secondary. When healthcare users grows, user can add block storage disks and attach them to created instance for adding more user to the system.

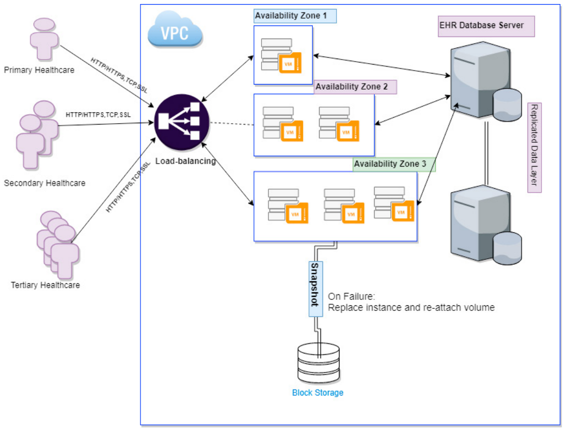


Fig. 4. High availability architecture for rural healthcare system

3.2.1. *Testing for sustainability of the system*

The network connectivity is ensured by using the dedicated high speed optical networks, which connects all rural facilities including sub centre, primary health centre and community health centre. The private/Hybrid cloud services are created by using co-locating our server in Data Center(Institute TIER IV Certified). With this network connectivity is attained in all levels of healthcare system.

4. Securing patient data in rural healthcare system

The following is a list of suggested countermeasures to address the security problems faced by rural healthcare organization.

4.1. *Dual database for securing the patient data*

The security model for storing and retrieving sensitive personal information of the patient are depicted in Fig. 5. The model consists of central health record server in communication with a medical record repository or database. The patient himself owns the contained data which are the sensitive personal data. The medical record of the patient which typically is found in such records may include several type of medical information such as biometric information, Physical, psychological and mental health condition, family history, allergies, medications taken, medical conditions, past medical treatments, and diseases. The medical records may further include financial information such as bank account or credit card or debit card number with identity of the patient. According to the IT Act, 2000 above medical record fields are considered as sensitive personal data information.

Ensuring the privacy, security, and confidentiality of Electronic Health Record has been considered as fundamental principle for the health information management (HIM) .The health information system mainly requires safeguards to ensure the data is available when needed and also to ensure that the information is not used, disclosed, accessed,

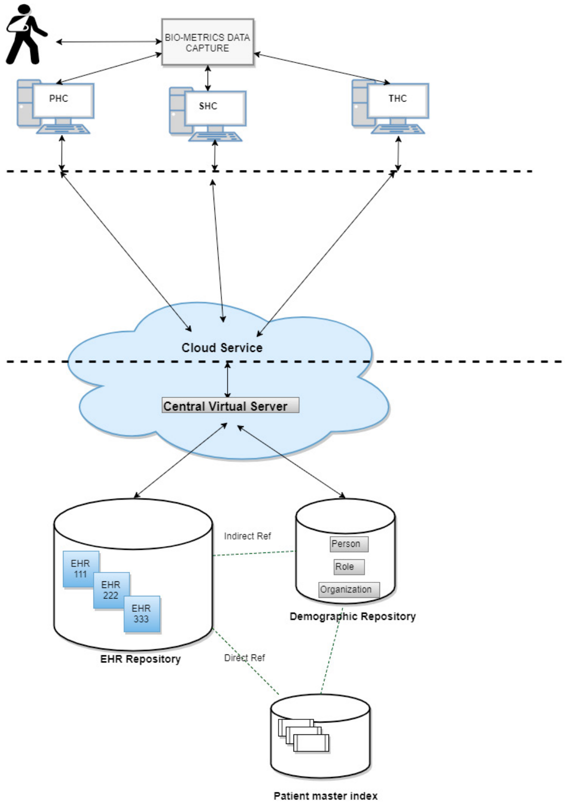


Fig. 5. Various actors interaction with EHR System

altered, or deleted inappropriately while being stored or transmitted. The Security Standards work together with the Privacy Standards to establish appropriate controls and protections. The medical record maintained in the medical record repository or database is identified using patient identification number. Health data of the patient are individually identifiable under mentioned identifiers. Information of the patient could be used either alone or in combination with other information.

The proposed system makes use of two database one for medical record and another for biometric information. Medical record database need not include personal identification of the patient (patient name) instead patient identification or biometric information is stored in the biometric database. Patient health information stored in the medical records may be identified using one or more identifier associated with the patient. Both the database are associated or linked by using an alphanumeric pass-code. Using this pass-code medical records can cross-reference with biometrics data. The patient data are available for the patient without using the patient's name or other personal information.

The virtual machine in the private cloud consists of databases to store the patient data. Private cloud infrastructure provides compute,storage and network services for managing the data. The interface between gateway and virtual machine database is shown in Fig. 6.

In dual database, to store the patient health information EHR database is used, in which data is stored in encrypted format. To store the key and hash value another database is used called key database. The main role is to perform encryption operation. In order to identify the key used for encrypting the data, the timestamp at which the operation is performed is also stored in the corresponding databases. Before storing data into the database, encryption is applied

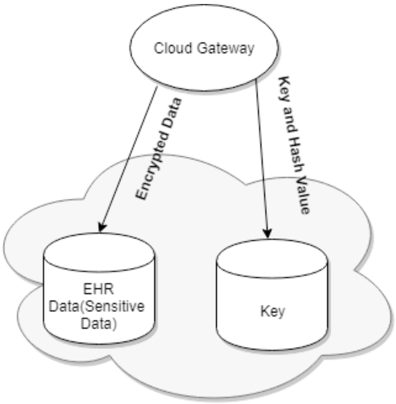


Fig. 6. Interface between gateway and VM Database

at the gateway to maintain confidentiality of the patient data. The encrypted data is hashed to perform integrity, which prevent from modification The hash value that is stored in the cloud is computed as:

$$H_i\{m\} = Hash(E_i(m)) \,||\, Key_i \tag{1}$$

where $H_i(m)$ is the hash value of the i^{th} data, E_i is the encrypted data and Key_i is the key used for encrypting the i^{th} data. Thus $H_i(m)$ maintains the integrity of the encrypted data and also the key used for performing the encryption. For decryption VM checks for the integrity constraint. If satisfied, the decryption operation is performed using the corresponding key. This decrypted information is forwarded to the service cloud. The service cloud displays the results in the required format to the end user.

In the proposed model for private cloud secure architecture we observe that before sending health data to cloud the encryption and the hash operations are performed. Actual data of health record is stored in one database and other contains the key required for performing the encryption. Hence, access to sensitive patient information from the cloud EHR database is blocked for an attacker. Therefore, the proposed architecture protects the sensitive information of the patient by maintaining the confidentiality and integrity of the data. As a result the healthcare users can access relevant information from anywhere and at anytime.

4.2. Authorization model for proposed private cloud model

Authorization services include policy management, role management, and role-based access control. Cloud based EHR system supports OAuth[23] for authorization as shown in Fig. 7. Authorization model contains four rows for representing user (browser), application, Authorization server and resource server. User or browser own the resources which is stored in the remote server or remote database. If user wants to access the resources, first he/she has to enter the credentials such as user-name and password.

User credential validation is done at the authorization server where after validation, it is redirected back to user for further access to the resources. On behalf of the user application, the token is obtained and returned to the application. Using this token, application talk to the resource server and get required data to access. The presentation page is displayed to the user to view the data. The elements of authentication services used for authorizing the health information resources are listed in Table 2. The cryptographic syntax used for the authorization is shown in equation 2.

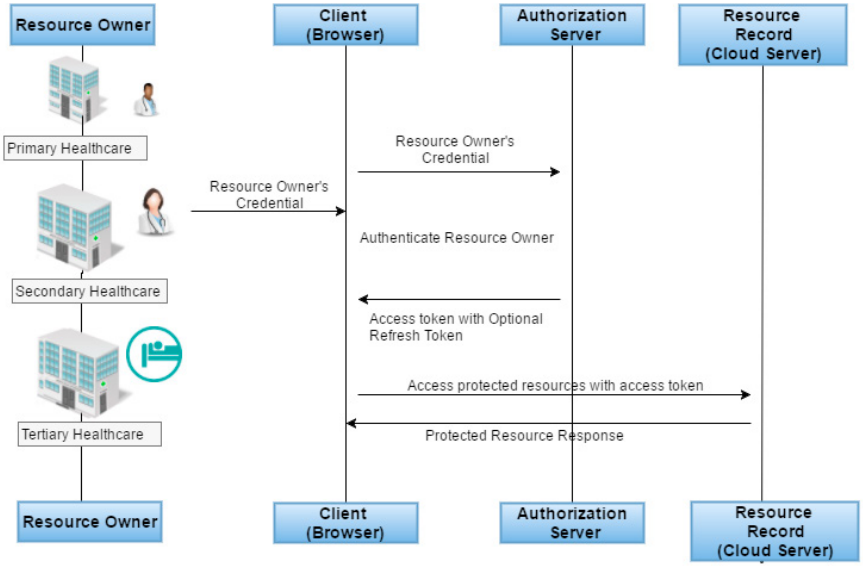

Resource Owner
Client (Browser)
Authorization Server
Resource Record (Cloud Server)
Primary Healthcare
Secondary Healthcare
Tertiary Healthcare
Resource Owner's Credential
Resource Owner's Credential
Authenticate Resource Owner
Access token with Optional Refresh Token
Access protected resources with access token
Protected Resource Response
Resource Owner
Client (Browser)
Authorization Server
Resource Record (Cloud Server)

Fig. 7. Authorization Model for healthcare system

$$\begin{aligned}
C \rightarrow AS &: Options \,||\, Id_c \,||\, Times \,||\, Nounce \,||\, Service \\
AS \rightarrow C &: Options \,||\, E[Id_c \,||\, Times \,||\, Nounce \,||\, K_{c,v}] \\
AS \rightarrow V &: Service \,||\, Options \,||\, Times \,||\, K_{c,v} \\
C \rightarrow V &: E[K_{c,v} \,||\, Message] \\
V \rightarrow C &: Nounce
\end{aligned} \tag{2}$$

Table 2. Elements of Authentication Service

Options	Designation	Healthcare level	Rural	Urban	Year of experience
Idc	Aadhar number				
Times	Used by the client to request the following time setting in the ticket. From: Start time for the requested ticket Till:Expiration time for the requested ticket rtime: requested renew -till time				
Nonce	A random value assure that the response is fresh.				

5. Results and Discussion

Rural hospitals are under more pressure than urban hospitals because of the size and scale of population and available infrastructure facilities. The field study was conducted for the hospitals at different levels namely Primary Healthcare Centre (PHC), Secondary Care Centre (SHC), and Tertiary Care Centre (THC) in Udupi district, Karnataka, India. With this study it is concluded that rural and community hospitals are having limited IT-infrastructure facility to manage and maintain the health information. For the following reason, private cloud model is developed to serve all the connected hospital in the udupi rural healthcare system. For this Faststart model of installation was used with Eucalyptus version 3.4.2 in Community health centre(CHC). All the necessary setup was done and an instance was launched with the custom Ubuntu Karmic (9.10) image. Then by accessing the instance from terminal using ssh, proper network settings like proxy settings, DNS servers were configured and the internet connection was given to the instance. With this setup CHC are allowed to access the resources and also using the same private cloud setup resource accesses are provisioned and provided access to the resources from outside the intranet (Internet). Private cloud implementation in CHC, shares the required resources to all rural health hospital on rent basis to deploy their health application on private cloud. By using this facility different levels of healthcare users can share information easily at any time they need.

For secure storage introduced security levels based on type of content and accessibility. In this approach different levels of security in cloud storage and access restrictions for the data is specified. From the web application, web log analysis is performed which parses the server log from a web server based on the number of times demographic data of the patient is accessed are stored in log file. The frequency of patient demographic data access is shown in the Fig. 8. In this 0 signifies low, 0.5 medium and 1 for high frequency of access. Based on that, security provisions are extended. Properties of demographic data to store in the cloud database with encryption is shown in Fig. 9

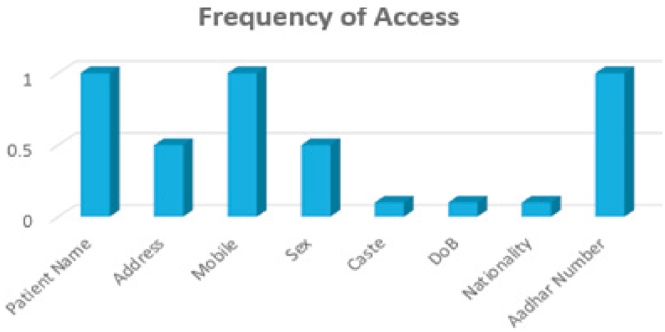


Fig. 8. Patient Demographic Data properties

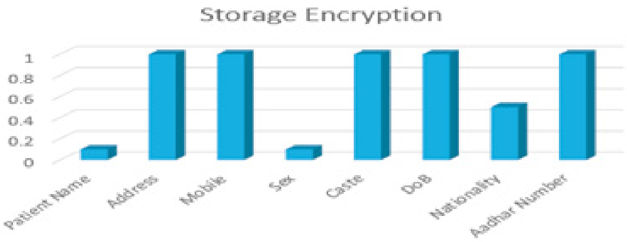


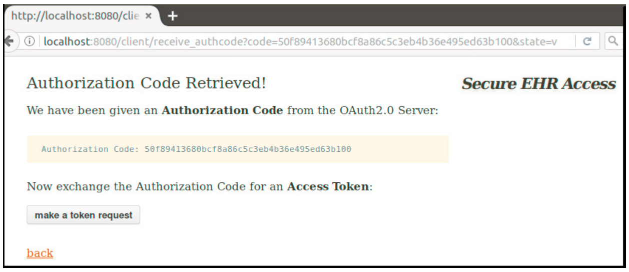
Fig. 9. Properties of demographic data to store in cloud database

In private cloud, authorization model implemented using OAuth method. In which healthcare user can access to computer or network resources which are regulated on the basis of authorization code and token. A healthcare user can have multiple resources stored in cloud database model. Various factors are considered when it comes to assign the authorization code and token generation. Once the criteria has been fulfilled, the user can access the resources.

The OAuth Server is created with following consideration:

- Authorize - Server endpoint which grants the EHR web application to an authorization code.
- Token - Server endpoint which grants the web application an access token when supplied with the authorization code using above step.
- Resource - Server endpoint which grants the web application access to EHR protected resources when supplied to the token.

Web application is created to access the healthcare resources from the server. If healthcare professionals wants to access resources of patient, user has to click the authorize button. Once he clicks, the request will go to EHR server where OAuth server is running. Once server receives the request, web application shows abstract view of the


http://localhost:8080/clie ×
localhost:8080/client/receive_authcode?code=50f89413680bcf8a86c5c3eb4b36e495ed63b100&state=v

Authorization Code Retrieved!

Secure EHR Access

We have been given an **Authorization Code** from the OAuth2.0 Server:

```
Authorization Code: 50f89413680bcf8a86c5c3eb4b36e495ed63b100
```

Now exchange the Authorization Code for an **Access Token**:

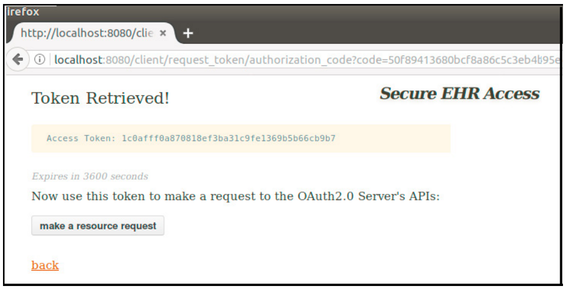
make a token request
back

Fig. 10. Authorization code is generated by the server

resources which healthcare user can access. After confirmation of the resource displayed in the screen, user has to complete authorization and receives an authorization code. For performing this user has to click the button called ”Yes, I Authorize The Request”.

Authorization code is generated by the server and code is exchanged with client as shown in Fig. 10. For example the authorization Code received is 675931b9e0137277c2891a64682d025a96850a95. With this code user can access the token by sending authorization code to server.

As soon as server receives the request , access token is generated with expiration time of 3600 seconds. For example access token is received d3291f6a495542d6029ba2f225a2374d4cbde74d. Using this token user makes request for the resources and user is redirected to the resource as shown in Fig. 11.


irefox
http://localhost:8080/clie ×
localhost:8080/client/request_token/authorization_code?code=50f89413680bcf8a86c5c3eb4b95e

Token Retrieved!

Secure EHR Access

```
Access Token: 1c0afff0a870818ef3ba31c9fe1369b5b66cb9b7
```

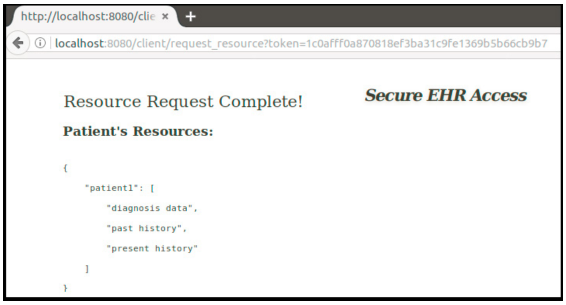
Expires in 3600 seconds

Now use this token to make a request to the OAuth2.0 Server's APIs:

make a resource request
back

Fig. 11. Access token is generated with expiration time

User can access the resources till token expiries. Example of resources accessed by user is shown in Fig. 12.


http://localhost:8080/clie ×
localhost:8080/client/request_resource?token=1c0afff0a870818ef3ba31c9fe1369b5b66cb9b7

Resource Request Complete!

Secure EHR Access

Patient's Resources:

```
{
    "patient1": [
        "diagnosis data",
        "past history",
        "present history"
    ]
}
```

Fig. 12. Access the health record resources till token expiries

6. Conclusion

Building private cloud is an extremely useful idea for rural healthcare sector to make data available in all levels of healthcare system. It makes the complete process of building a private cloud infrastructure very easy if the approach is standardized. Therefore, rural healthcare organizations should move towards building their own private cloud infrastructure which could be an excellent solution for the countrys needs to have improved Health care in rural areas. Building a community private cloud becomes much simpler if an accurately organized method is followed to do so. Once standardization is achieved, additional automation can be used to further shorten process times. In the cloud computing environment, the privacy of the electronic health data is a serious issue that requires a special consideration. The proposed solution in this paper provides authentication and storage model strengthen user health data when data is stored in the cloud environment. Use of two different database for medical record which blocks the path for an attacker to modify the data stored in the cloud. Future work with respect to the RBAC model would be to implement cryptographic algorithms and integrate it with the system to guarantee entity authentication and thus further increase the security.

References

1. Dasgupta, R., Qadeer, I., et al. The national rural health mission (nrhm): a critical overview. *Indian J Public Health* 2005;**49**(3):138–40.
2. Huffman, E.K.. *Medical record management*. Physicians' Record Company; 1972.
3. Mohrman, S.A., Shani, A.B.. *Reconfiguring the eco-system for sustainable healthcare*. Emerald Group Publishing; 2014.
4. Fraser, H., Biondich, P., Moodley, D., Choi, S., Mamlin, B., Szolovits, P.. Implementing electronic medical record systems in developing countries. *Journal of Innovation in Health Informatics* 2005;**13**(2):83–95.
5. Srinivasa, D., Siddegowda, Y., et al. Rural health care towards a healthy rural india: A social work response. *Asian Journal of Development Matters* 2018;**12**(1s):68–74.
6. Singh, P., Kathuria, R.. Infrastructure and connectivity in india: getting the basics right. *Asian Economic Policy Review* 2016;**11**(2):266–285.
7. Skilton, M., Director, C.. Building return on investment from cloud computing. *White Paper, The Open Group* 2010;.
8. Pooja, B., Pai, M.M., Radhika, M.P.. A dual cloud based secure environmental parameter monitoring system: A wsn approac. In: *International Conference on Cloud Computing*. Springer; 2013, p. 189–198.
9. Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., et al. The eucalyptus open-source cloud-computing system. In: *Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on*. IEEE; 2009, p. 124–131.
10. Sun, Y., Zhang, J., Xiong, Y., Zhu, G.. Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks* 2014;**10**(7):190903.
11. Latif, R., Abbas, H., Assar, S., Ali, Q.. Cloud computing risk assessment: a systematic literature review. In: *Future Information Technology*. Springer; 2014, p. 285–295.
12. Aceto, G., Botta, A., De Donato, W., Pescap, A.. Cloud monitoring: A survey. *Computer Networks* 2013;**57**(9):2093–2115.
13. Wang, P., Ding, Z., Jiang, C., Zhou, M.. Design and implementation of a web-service-based public-oriented personalized health care platform. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 2013;**43**(4):941–957.
14. Birke, R., Podzimek, A., Chen, L.Y., Smirni, E.. Virtualization in the private cloud: State of the practice. *IEEE Transactions on Network and Service Management* 2016;**13**(3):608–621.
15. Freet, D., Agrawal, R., Walker, J.J., Badr, Y.. Open source cloud management platforms and hypervisor technologies: A review and comparison. In: *SoutheastCon, 2016*. IEEE; 2016, p. 1–8.
16. Daman, R., Tripathi, M.M., Mishra, S.K.. Security issues in cloud computing for healthcare. In: *Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on*. IEEE; 2016, p. 1231–1236.
17. Khan, M.F.F., Sakamura, K.. Context-aware access control for clinical information systems. In: *Innovations in Information Technology (IIT), 2012 International Conference on*. IEEE; 2012, p. 123–128.
18. Yu, S., Wang, C., Ren, K., Lou, W.. Achieving secure, scalable, and fine-grained data access control in cloud computing. In: *Infocom, 2010 proceedings IEEE*. Ieee; 2010, p. 1–9.
19. Xiao, Z., Xiao, Y.. Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials* 2013;**15**(2):843–859.
20. Yu, S., Wang, C., Ren, K., Lou, W.. Attribute based data sharing with attribute revocation. In: *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*. ACM; 2010, p. 261–270.
21. Koufi, V., Malamateniou, F., Vassilacopoulos, G.. Ubiquitous access to cloud emergency medical services. In: *Information Technology and Applications in Biomedicine (ITAB), 2010 10th IEEE International Conference on*. IEEE; 2010, p. 1–4.
22. Xiao, Z., Xiao, Y.. Security and privacy in cloud computing. *IEEE Communications Surveys & Tutorials* 2013;**15**(2):843–859.
23. Kasthurirathne, S.N., Mamlin, B., Kumara, H., Grieve, G., Biondich, P.. Enabling better interoperability for healthcare: lessons in developing a standards based application programing interface for electronic medical record systems. *Journal of medical systems* 2015;**39**(11):182.