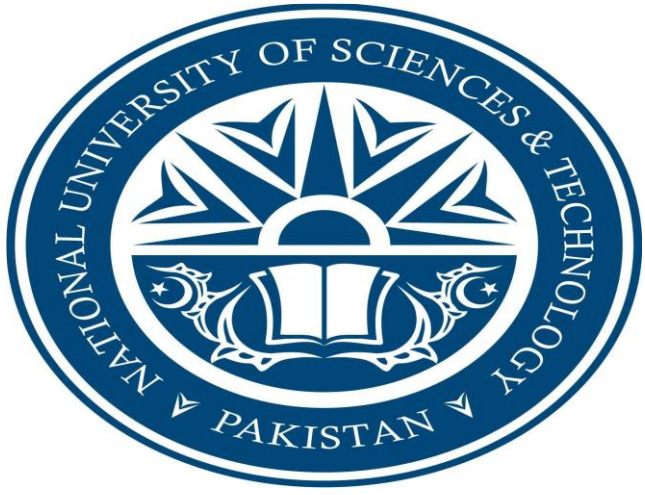
SECURE ARCHITECTURE FOR EMR



By

Waqar Ahmad

2011-NUST-MS-CS-27

Supervisor

Dr. Abdul Ghafoor Abbasi

SEECS NUST

A thesis submitted in partial fulfillment of the requirements for the degree

of MSCS

In

School of Electrical Engineering and Computer Science,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(June 2015)

Approval

It is certified that the contents and form of the thesis entitled “Secure Architecture for EMR" submitted by Waqar Ahmad have been found satisfactory for the requirement of the degree.

Advisor: Dr Abdul Ghafoor Abbasi

Signature:_____

Date: _____

Committee Member1: Dr Nauman Qureshi

Signature_____

Date:_____

Committee Member2: Dr Awais Shibli

Signature _____

Date: _____

Committee Member3: Muhammad Qaiser Chaudary

Signature _____

Date: _____

CERTIFICATE OF ORIGINALITY

I here by declare that the research paper titled "***Secure Architecture for EMR***" my own work and to the best of my knowledge. It contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST or any other education institute, except where due acknowledgment, is made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST or elsewhere, is explicitly acknowledged in the thesis.

I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic is acknowledged. I also verified the originality of contents through plagiarism software.

Author Name: Waqar Ahmad

Signature: _____

Acknowledgment

I am very thankful to my **Advisor Dr Abdul Ghafoor Abbasi** for his guidance, supervision, help on this research and constant encouragement. You are a true mentor and role model for me.

Also I would like to thank my family for love and support. Special thanks to my **Mother** I could not have done this research without your prayers.

Table of Contents

List of Abbreviations

Abbreviations	Description
EMR	Electronic Medical Record
SaaS	Software as a Service
Paas	Platform as a Service
IaaS	Infrastructure as a Service

List of Figures

List of Tables

Abstract

With the advent of virtualization, high speed availability of internet and distributed computing techniques make computing resources cheaper, more dominant and more available than ever. Most of the world business shift from traditional IT systems to new computing model in recent years and this new computing model is called cloud computing. The new model offers new features to healthcare domain to enhance their functionality. So this domain is shifting rapidly from traditional computing to cloud computing. In healthcare domain different stakeholders like physicians, insurance companies, patients, healthcare providers need to work together. For information processing/sharing among different stakeholders cloud computing is best option in terms of cost, time, throughput and service uptime. Shifting from traditional EMR system to cloud implies that there are several threats in terms of security and privacy. This is main barrier because of which healthcare industry feel hesitation to transform its services on cloud.

In our research we propose a secure architecture for the EMR. Authentication service implemented using extended FIPS 196 authentication protocol. i.e before exchanging sensitive information on cloud between client and server, must exchange random numbers and generate/verify digital signatures. Once authenticated a user, then at every call checked that user has required permissions to access a resource on EMR or not. For this purpose specific policy decision point implemented that decides access or rejection for that particular resource on EMR.

Chapter 1

INTRODUCTION

This chapter will introduce the topics electronic medical record (EMR) and cloud computing, advantages of cloud computing with respect to EMR, cloud computing issues with respect to EMR, problem statement, thesis contribution and thesis organization.

1.1 Electronic Medical Record and Cloud computing

From digital information age inception, new and new advancement introduced day by day. This advancement affect every field of life. Health is one of the field. If we talk about specifically technologies advancement in healthcare field. These technology advancement have large spectrum from surgeries to medicine, paper based prescription to digital prescription etc. Electronic medical record or EMR is digital information about a patient. These digital information include patient personal data, laboratory tests, radical images like medical resonance image results, x-rays etc. With the development of traditional EMR systems did not fulfil the requirements of today health care needs. Today health care industry required the model which should be information-centric because different stakeholders need cooperation and collaboration in order to improve health care facilities and allow the use of different standards for cooperation, collective functioning and for information sharing. So cloud computing is best candidate for such requirements. The name "cloud computing" taken from cloud symbol as this symbol represent internet on diagrams. Generally "cloud computing" used for anything which participate for providing hosting services. Contrary to traditional hosting cloud service has three properties that is, sold on pay per use, flexible and have service provider. In today global world cloud computing has its own importance. For information processing/sharing among different stakeholders cloud computing is best option in terms of cost, time, throughput and service uptime. Other factors which make cloud computing for health care industry most interested choice, are high speed availability of internet, distributed computing and virtualization.

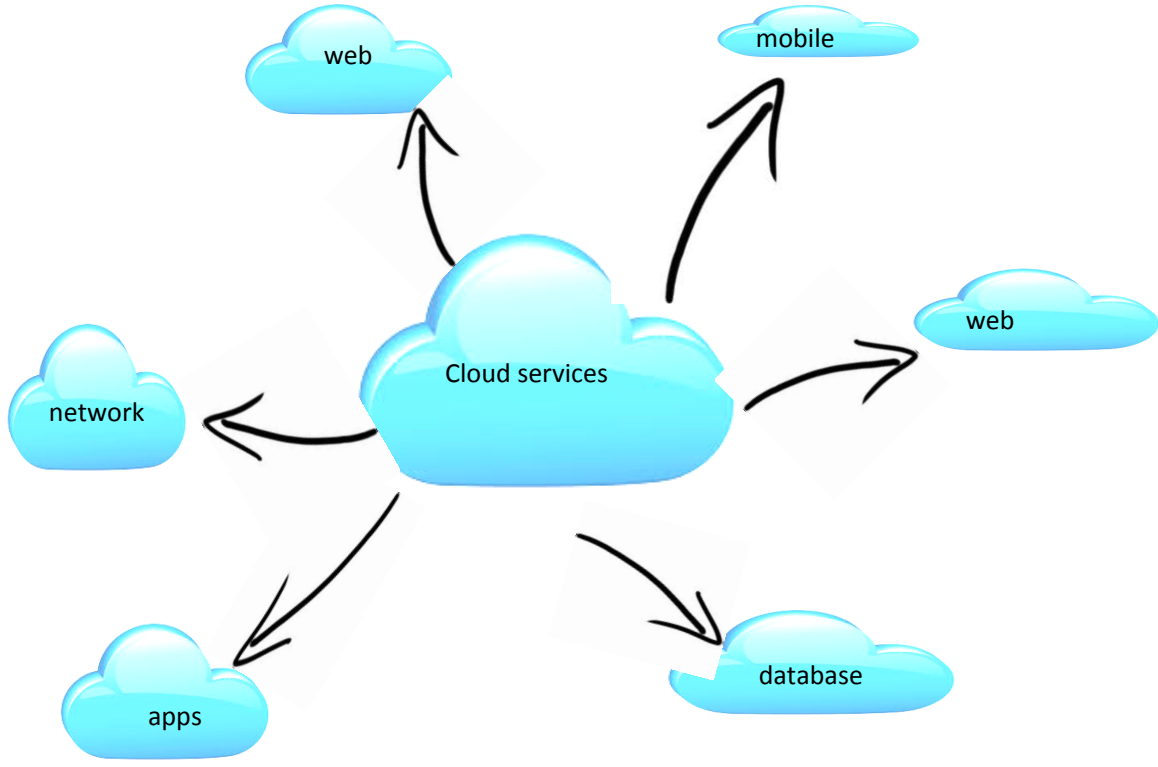
Different cloud models implemented for EMR 1) Software as a service 2) Infrastructure as a service 3) Platform as a service

Software as a service is from end user point of view. Software and hardware are residing on the cloud and usually connects the applications via internet using some browsers. Provisioning of resources is the responsibility of SaaS provider. Examples of SaaS providers are CureMD and bizMatics etc.

Platform as a service is from developer point of view. This type of service provide full fledge environment for development of cloud applications without the headache of buying underlying software, hardware and hosting services. AmerisourceBergen is an example of private PaaS.

Infrastructure as a service is pay per use basis. Cloud providers provide data centers. Users of this model pay for the storage, maintenance and computation. Example of PaaS provider is Amazon Web services.

Figure 1.1 Cloud Services



Different EMR cloud deployment models also used 1) Private cloud 2) Public cloud and 3)Hybrid cloud.

Public cloud is where vendors provide, managed and owned services (hardware, software, supporting infrastructure) to organizations on affordable prices. Clients do not need to purchase software, hardware and supporting infrastructure.

Private cloud is managed and operated by a single company and actually this company decides the proper way in which virtualized resources and services are made especially for different business group's needs.

Hybrid cloud use mixture of public cloud and private cloud.

1.3 Advantages of EMR cloud computing

In traditional EMR environment installation of physical equipment on the owner in-house office increases cost and on the other hand cloud might provide with comparatively less cost.

Cloud computing provide high computing facility and large storage capacity. Those facilities are absent in traditional EMR environment. Cloud services also allow EMR owners to more concentrate on their business rather than worry about data storage space and hiring technical staff to maintain software. It also eliminates the cost for purchasing physical hardware and also saves technical persons (to maintain the hardware) cost. Cloud computing also saves energy. The customers of cloud also free from maintenance headache. This maintenance is responsibility of owner of the cloud service. Cloud services are more stable than local in-house services. i.e cloud services uptimes are higher than local given services. Cloud computing gives the advantage of doing work collaboratively, working different cultures people and sharing documents among the employees of an organization. A patient can check its information on smart phones, tablets any time anywhere. Different health care providers can exchange information under certain rules and regulations. With passage of time different protocols or standards developed for exchanging health care information among the health care entities. Major example of such type of standard is HIPPA. Cloud computing also allows us to working on shared repositories if this technology was absent then people would communicate or working through different phenomena like emails etc. Those traditional methods do not as fast as cloud services. If we take example of shared repositories which are getting huge interest from users. If we remove cloud computing from this phenomena then people working on repository in different locations of the world then that repository would have different versions and different formats. Those people would communicate through email and this method require more time. But cloud computing allows shared repository. People work on shared repository simultaneously and communicate through instant soft wares like chat etc. another advantage of using cloud is data storage on central location. One recent study shows that only on airports around 8 lakh laptops stolen every year [business week July 5, 2011] if data stored on cloud then it is not an issue that the hardware stole really impact on data. Continuously data backups taken by SaaS provider so that if on one region server fail then SaaS provider restore the data from other region server. EMR data mostly comprise on x-rays, MRIs, lab tests etc. Those data require large space for storage. These storage provide by cloud comparatively on less cost. So this point is another reason of health care industry shift on cloud. Cloud computing also provide facilities to different health care systems to share information among each other in more timely fashion

and eliminate duplicate testing. Another facility provide to health care industry by cloud is the ability for tracking and analysis of data.

In recent surveys shows that cloud has 30% money budget of the total IT budget. Cloud computing industry grew with worth 45 billion US dollars in 2012 and it is expected that in 2017 the cloud industry will grow to 117 billion US dollars. [by Chloe Morrison, nooga.com, November 26, 2013]

1.4 EMR Cloud computing issues

Health care cloud services gives advantages but also have some downsides for example user lose control on the data if user want to kept data private. Another downside is owner of the cloud can use cloud users data for their own businesses as well for example data mining purposes. Health care industry need data security, privacy, data access trace and access of the data authorization according to some rules and regulations. Traditional EMR systems when move to cloud then we can divide health care applications in two categories 1) clinical applications 2) nonclinical applications. Example of clinical applications comprise upon software for radical images of the patient, blood tests and EMR of the patient while nonclinical applications comprise on automatic bill generation, financial accounting etc. Moving towards cloud for above type of applications ultimately change the level of privacy and security. For example EMR data is more sensitive than the automatic bill generation application data. So EMR data privacy and security level will be very high as compared to bill generation application data. Another big issue for cloud adoption is interoperability problem among different health care providers. Now a day's different standard developed for interoperability problems. For example HL7.

When healthcare related data stored on cloud then along with privacy issue, it is also a juridical issue so that's why different standards developed for EMR. One of the most famous standard published for EMR is Health Insurance Portability and Accountability Act. (HIPAA). This standard gives the guidelines for the data confidentiality. National Institute of Standards and Technology (NIST) published series of standards one of them is Federal Information Processing Standards or FIPS. FIPS gives guidelines for the entities authentication which want to authenticate each other prior to data exchange. FIPS is based upon public key cryptography.

1.5 Problem statement

Health care data need confidentiality, privacy and security. These are most important concerns and challenges towards health care cloud adoption. For EMR system provide a secure architecture and authentication protocol. The authentication process is derived from FIPS NIST 196 authentication protocol.

1.6 Thesis Organization

Following are the thesis organization

Chapter 2 is about the literature review.

Chapter 3 is for detailed design.

Chapter 4 is for implementation details.

Chapter 5 is for conclusion and future work.

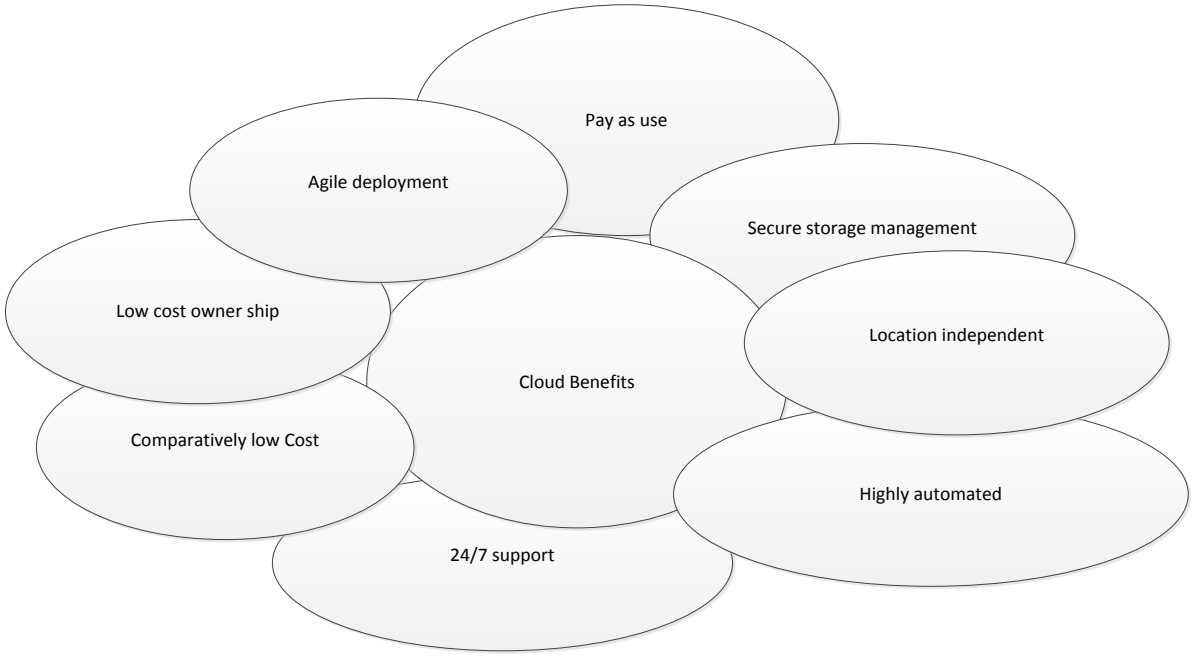
Chapter 2

Literature Review

2.1 Healthcare Cloud Computing

Cloud computing has become an emerging technology which changed the landscape of business and technology. In recent days, clients are running and accessing their applications from pool of virtualized computing resources available on different clouds. Below figure describes the major advantages of cloud computing

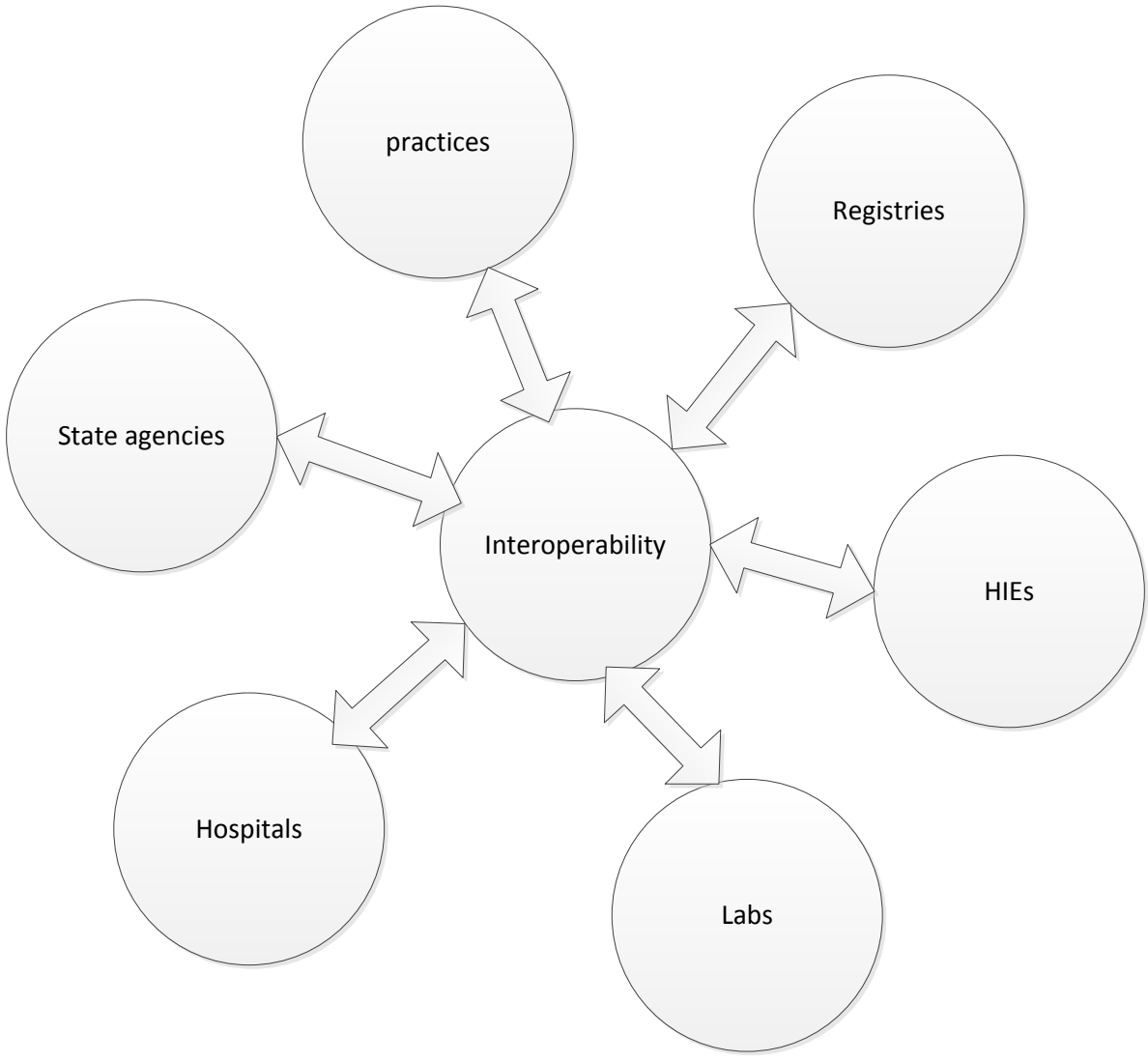
Figure 2.1 Healthcare Cloud Benefits



Now a days most of the world try to use cloud computing. New systems developed for different purposes. For example we use document sharing software. One of them is google drive. Like other fields health care industry also transfer its services from ordinary systems to cloud based systems[1]. e.g developed applications which can be run any platform like android operating system, windows platform and run on different devices anywhere anytime. Recently one more step achieved beyond the health care cloud adoption. That step is development of testing tools for healthcare applications integration. For example to share information among different health care stakeholders (industry, health authorities, developers, IT experts) different organizations work for this purpose. Integrating the Health Care Enterprise [2] is one of organization which actually created a process in which

interoperability among different IT systems improved. It makes basically those system operable which follow some health care standards for example HL7.

Figure 2.2 Healthcare Cloud Interoperability



We can divide healthcare into different domains like electronic health records, bioinformatics and clinical systems. These fields further divided with respect to different deployment models like private, hybrid and public clouds or divided with r[3] respect to different services models like Saas, Paas and Iaas etc. Cloud based market more and more popular day by day. It is shown from different surveys that cloud market reached more than 100 billion in 2013 with 20% increase in every year [4].

Many organizations want to switch on cloud computing. If we specifically talked about healthcare industry, this field has shortage of expert persons, second thing is services which are very costly [5]. As we know that diseases are more complex. Healthcare industry want to use modern technologies which should be cost effective and it should be suitable for the small to medium enterprises (as majority of healthcare enterprises belong to small to medium level). Those companies/ hospitals which did not adopt modern technologies and poor performance, in competitive environment kicked out from the market very quickly. Healthcare IT industry grows from departmental level to enterprise level. Because criticality of this domain, it needs redundancy of data, fast communication infrastructure and it should be cost effective. Cloud computing provide that infrastructure on comparatively low cost. Imagine how it will be costly if an organization created whole infrastructure. Cloud providers provide data centers, software for communication and computing infrastructure. Healthcare providers transfer their services to cloud vendors which reduces the headache of healthcare providers. This way is very cost effective for healthcare providers as maintenance and operations are responsibilities of cloud providers [6]. Cloud computing give advantages to this industry as it provides centralized location for sharing data to different stakeholders.

Different stakeholders are 1) Laws enforcement agencies 2) Government 3) Research institute 4) Insurance companies 5) Hospitals 5) Pharmacies

Healthcare cloud computing have several advantages 1) Cost effective 2) Sharing of data 3) Healthcare quality improvement 4) Research improvement.

Cloud computing provide high computing facility and large storage capacity. Those facilities are absent in traditional EMR environment. Cloud services also allow EMR owners to more concentrate on their business rather than worry about data storage space and hiring technical staff to maintain software. It also eliminates the cost for purchasing physical hardware and also saves technical persons (to maintain the hardware) cost. Cloud computing also saves energy. The customers of cloud also free from maintenance headache. This maintenance is responsibility of owner of the cloud service. Cloud services are more stable than local in-house services [7]. i.e cloud services uptimes are higher than local given services. Cloud computing gives the advantage of doing work collaboratively, working different cultures people and sharing documents among the employees of an organization. A patient can check its information on smart phones, tablets any time anywhere. Different health care providers can exchange information under certain rules and regulations. With passage of time different protocols or standards developed for exchanging health care information among the health care entities. Major example of such type of standard is HIPPA. Cloud computing also allows us to working on shared repositories if this technology was absent then people would communicate or working through different phenomena like emails etc. Those traditional methods do not as fast as cloud services. If we take example of shared repositories which are getting huge interest from users. If we remove cloud

computing from this phenomena then people working on repository in different locations of the world then that repository would have different versions and different formats. Those people would communicate through email and this method require more time. But cloud computing allows shared repository. People work on shared repository simultaneously and communicate through instant soft wares like chat etc. another advantage of using cloud is data storage on central location. One recent study shows that only on airports around 8 lakh laptops stolen every year [business week July 5, 2011] if data stored on cloud then it is not an issue that the hardware stole really impact on data. Continuously data backups taken by SaaS provider so that if on one region server fail then SaaS provider restore the data from other region server. EMR data mostly comprise on x-rays, MRIs, lab tests etc. Those data require large space for storage. These storage provide by cloud comparatively on less cost. So this point is another reason of health care industry shift on cloud. Cloud computing also provide facilities to different health care systems to share information among each other in more timely fashion and eliminate duplicate testing. Another facility provide to health care industry by cloud is the ability for tracking and analysis of data.

When we talk about patient data sharing then it means that there should be some standards which will comply for patient data protection and interoperability standards among the providers [8]. When data exchange among different healthcare providers there should be some data types and formats according to which data exchange. The sensitive information sharing require rules and regulations for the privacy of patient data. Other threat is using patient data without permission from patient by third parties for data mining purposes. It is broadly accepted that privacy of user information is major concern in health care industry.

In cloud computing with respect to healthcare industry there are different cloud providers, different cloud consumers, cloud services used by cloud consumers, High security risks with this kind of environments of data sharing [9]

1) Very difficult when different healthcare consumers' data store in a single place.
2) Above environments require strong authentication and access control mechanisms.

Privacy is another issue along with security and this is main barrier because of which healthcare industry feel hesitation to transform its services on cloud. This concern is how to secure data 1) From other patients 2) From other healthcare providers 3) From other cloud providers.

Healthcare providers, patients and other stakeholders seek solutions for privacy of information which should be enough and can be accepted by all stakeholders.

2.2 Healthcare challenges on cloud w.r.t security and privacy

Besides major advancements in cloud computing technology, several challenges have been faced which need great attention [10]. One of the basic issue for healthcare industries to

transfer on cloud is privacy and security. Because they have sensitive data of patients security and privacy are the major concerns. Different laws formed for security and privacy on cloud. For example health information portability and accountability act also known as HIPPA. This law enforce healthcare providers to implement policies which make these sensitive information secure and private and inform users when any privacy and security compromised. Few challenges are 1) Data cannot accessed by unauthorized person. 2) Integrity of data. 3) Authentication 3) Privacy of the data. 4) Data safety and healthcare data monitoring.

It is need to separate the challenges on the basis of domain [11]. For example to solve that issue it is main point to observe that either it is cloud computing problem or it belongs to healthcare specifically. Different strategies adopted to solve privacy and security problems. One approach used in this regard is called patient-centric approach in which it is the responsibility of the EMR owner that he/she allow the access to data to others. First owner encrypt data and then share the data to authorized people [16]. The encryption based upon attributes and distribute keys to authorized people. This approach impose overhead upon the EMR owner rather than cloud owner[12]. This approach did not solve privacy and security issues for the cloud owner. To overcome previous strategy issues new strategy introduced that rather to overload EMR owner side with heavy computation, shifted to cloud owner side using access control without giving data in plain text form. This approach done using advanced techniques for data encryption 1) Key policy attribute based encryption 2) Proxy re-encryption 3) Lazy encryption

Records associated with attributes. Access structure created on the basis of set of attributes and each user associated with access structure. Both key policy attribute based encryption and proxy re-encryption at once used for EMR owner in order to computation operations delegation of the data without actual data disclosure to cloud owner. This approach achieve the privacy of the healthcare data. For scalability lazy encryption used.

DACAR [1] system developed with most common requirements achievement. This approach achieved following goals. 1) Identity verification using cryptography protocols. 2) Role based policies for resource access. 3) During operation assure data completeness, consistency and accuracy. 4) Auditing of data.

Techniques used for achieving above goals are following 1) Digital signatures.
2) Encryption and hashing. 3) Mapping identities. 4) Data integrity check sums.

Above approach has some drawbacks as it is also patient-centric. Some are listed below.
1) Increase responsibility on patient. 2) Process awareness required for the patient and it is most difficult part for patient. 3) In the case of emergency or in situation when patient not able to permit the access then who will be responsible for data access?

To minimize user overhead responsibilities can be moved to EMR service provider but this approach have trust and control problem [13]. Handling bunch of the records it also over headed to provider. If responsibility transfer from service provider to cloud provider then again problem arise for user lost control upon its privacy. So approaches should be adopt that overcome the issues or at least minimize to acceptable level. One possible solution is responsibility distribution. i.e distribute the responsibilities among the patients, service providers and cloud providers and devise a solution that is appropriate for all stakeholders.

Cloud computing provides a virtual infrastructure to its customers, so the privacy and security mechanism should be so flexible so that the customers have full control to protect their sensitive data. PasS (Privacy as a Service); a security mechanism for the customer data in cloud computing environment has been presented in [14]. It allows the users to protect, store, process and audit the confidential data by applying cryptographic co-processors by using PasS the user is able to configure software protection and data privacy and also PasS provides a useful feedback on applied privacy mechanisms which increase the customers trust in obtaining the cloud service for their data. Three trust levels; full trust, compliance-based trust and no trust have been applied on customer data depending upon the sensitivity of the data. A cryptographic coprocessor in PasS is the main device that is fully equipped with software and hardware requirements for the privacy and security of confidential data.

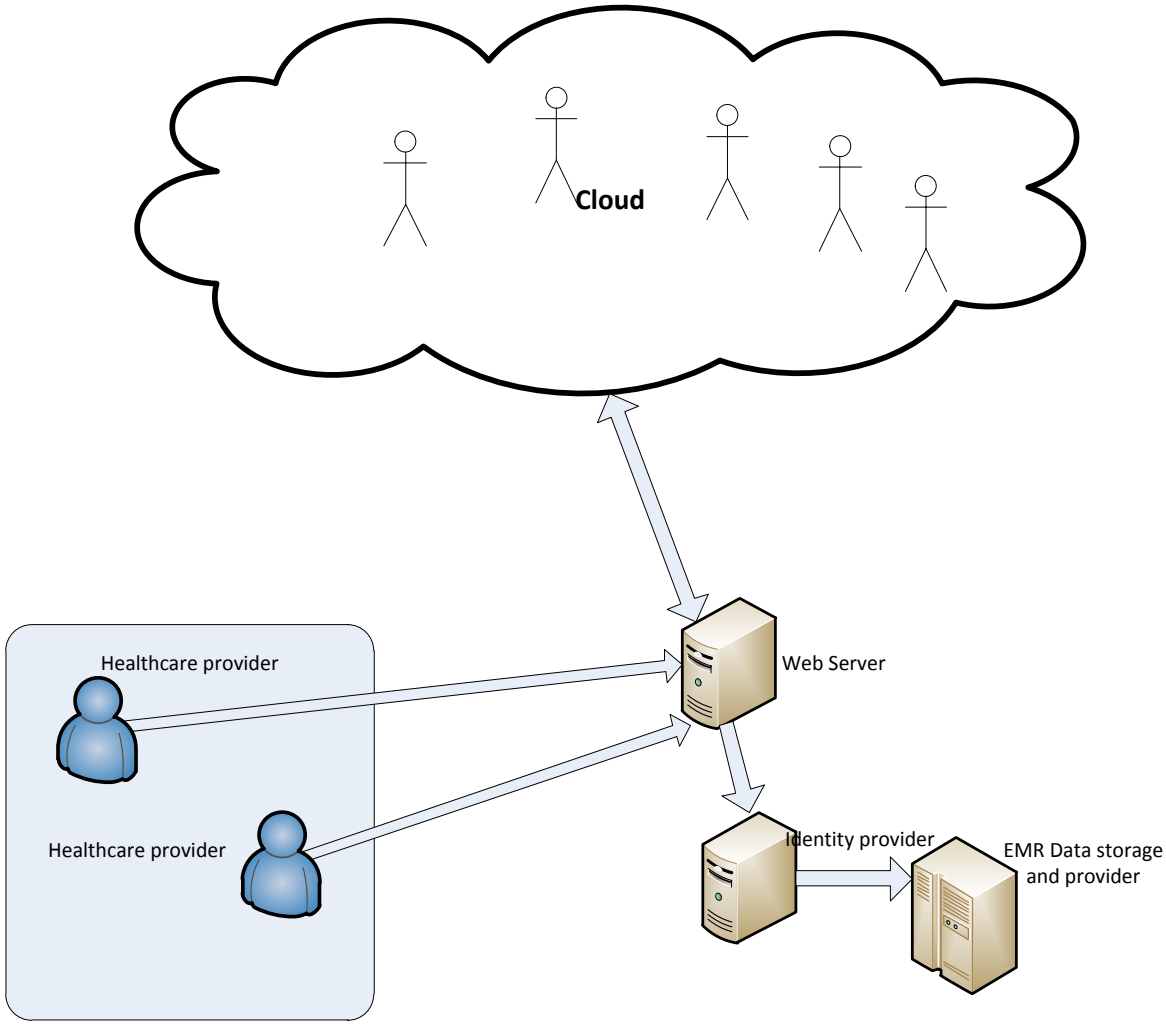
Most of the healthcare systems use different approaches on cloud for authentication and authorization. Username/password approach for authentication and role based access control for authorization mostly used. Apart from that role based access control approach some systems used artificial intelligence approach. i.e train the system with passage of time about a user which access some resources more and more. On the base of that hypothesis system learnt, make decision and make new constraints as well.

Cloud computing architecture has been employed in public health sector to fulfill the requirements of medically underserved populations with the help of Health ATM [15]. The health information from cloud computing environment is sent through Health ATM kiosks installed across community health clinics. The need for health management resources on cloud is based on the findings discussed in [15].

We are more concerned with privacy of the healthcare systems [16]. In a Cloud environment smartphone also used. Different authentication approaches used for security purpose between smartphone and cloud. Distributed computing building design gives a legitimate administration to impart conveyed assets and administrations all through the world by means of machine network. This construction modeling offers three principle characteristics. What's more today's Smartphones are better with this construction modeling, particularly with laas due to its little stockpiling limit. Cell phones have gotten to be very nearly machine and these can be seen as a small scale of PC. Since distributed computing offer dispersed information by means of system in the open environment in this way, there may happen security issues. To address this issue, this paper has proposed another information security

approach for Smartphone in distributed computing construction modeling, which guarantees secured correspondence framework and concealing data from others. Security level is kept up utilizing the Global Positioning System (GPS) and system supplier which guarantees solid client confirmation to secure our cloud. In cloud environment, assets are imparted among the greater part of the servers, however clients don't have the foggiest idea about the way that how their information are put away in the server. Traditional authentication scheme as shown below.

Figure 2.3 Existing Authentication Scheme



The ABI Research accepts that the quantity of portable distributed computing clients is

required to develop from 42.8 million (1.1% of aggregate mobile clients) in 2008 to 998 million (19% of aggregate mobile clients) in 2014. The security dangers have turned into an obstacle in the fast flexibility of the portable distributed computing engineering [17]. Critical endeavors have been given in exploration associations and the scholarly world to securing the versatile distributed computing engineering. In this paper we proposed a lightweight verification convention for portable cloud environment. Our proposed convention has numerous points of interest, for example, supporting client secrecy, nearby confirmation furthermore safety against related assaults, for example, replay assault, stolen verifier assault, adjustment assault, server mocking assault et cetera.

Normally the elements like user and services need to validate themselves to service providers (Sps) so as to utilize their administrations [18]. A substance gives personally identifiable information (PII) that interestingly distinguishes it to a SP. In the conventional application-driven Identity Management (IDM) model, every application keeps hint of characters of the elements that utilization it. In distributed computing, elements may have various records connected with diverse Sps, or one SP. Security in distributed computing is the capacity of a client or a business to control what data they uncover about themselves over the cloud or to a cloud administration supplier, and the capacity to control who can get to that data.

With the development and application of cloud computing, cloud storage is becoming more and more popular with many organizations, but traditional principal-minor structure for cloud storage is at risk of single point of failure. Moreover, it has brought safety risk. Cloud storage security has become the key problem of restricting the development of cloud computing. The paper has a deep research of cloud storage structure and cloud storage security, proposes a entity authentication protocol for P2P cloud storage [19] based on ternary Huffman Merkle hash tree (HuffMHT). This method using the concept of ternary HuffMHT can obtain an effective safe strategy. At the same time, symmetrical key algorithm and public key algorithm are just combined to reduce the authentication delay effectively and increase the network lifetime and enhances the security of the networks. Moreover, signatures of knowledge is used in this paper, which notes number of hash is reduced, the power which notes consume is debased, the network load is decreased. The performance of the system is discussed, and the encryption method has high efficiency and high security.

Chapter 3

Design

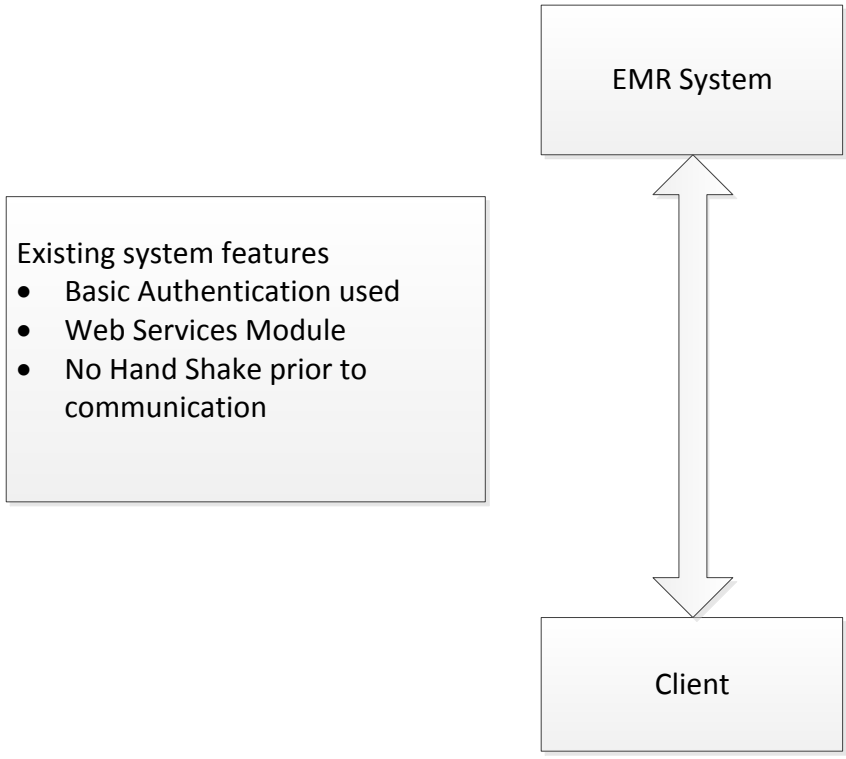
Health care data privacy and security is major concern when we talk about electronic medical records on the cloud. For EMR system provide a secure architecture

3.1 Proposed Design

Our proposed design will work as

Build a front end module where actually authentication will done. The added actually perform authentication and authorization process. The client can be an android phone, computer system etc. The steps used for this process as follows 1) Initial handshake before any sensitive data communication. 2) Secured communication 3) Use extended FIPS 196 NIST mutual authentication protocol. We use an EMR system for our process. An EMR system which currently provide basic authentication mechanism only and expose web services module for accessing data. Basic Authentication (BA) is a process in which no handshake done prior to looking forward this means that static http headers used for communication. The BA system gives no privacy insurance to the transmitted qualifications. They are just encoded with Base64 in travel, yet not scrambled or hashed at all. Essential Authentication is, thusly, regularly utilized over HTTPS. In basic authentication header must send with every request, to maintain user credentials for a certain time there is need to store credentials for user to continue its work smoothly. The current architecture as shown on following diagram

Figure 3.1 Current Design

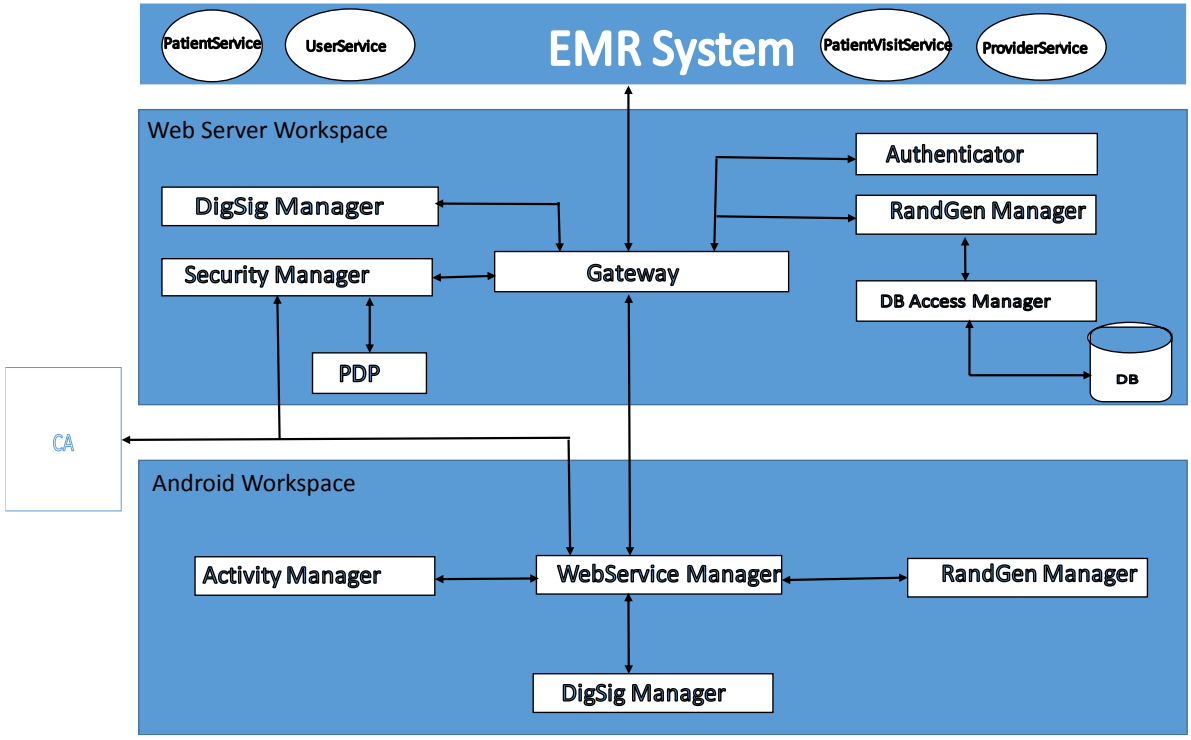


Existing system features 1) Basic Authentication used 2) Web Services Module 3) No Hand Shake prior to communication

The stakeholders of the authentication process must be able to use/generate digital signatures, random numbers and public/private key pair such that private key must be kept secure on local side and it will not transmitted on the network

High level diagram as shown

Figure 3.2 Proposed Design



The authentication/authorization process use following steps:

1) Android start an activity which is under the activity manager (AM)
2) AM call web service manager (WSM) given the ip address of the web server.
3) WSM create a proper format for IP address then encrypt it and send to web server.
4) Gateway receive that message and forward that message to security manager.
5) Security manager sent back the message after decryption to Gateway.
6) Gateway check the message sequence number if it is 1 then request to RandGenManager for random number generation.
7) RandGenManager generate random number and request for save number in DB with the help of Data Access Manager. Then that number also return to Gateway.

8) Gateway format a message with server random number, server ip address, increase message sequence number and forward to security manager.

9) Security Manager encrypt that message and sent back to Gateway.

10) Gateway forward that encrypted message to WSM on android.

11) WSM decrypt that message and determine message sequence number and request RandGenManager for generation of random number. RandGenManager save that number locally and send back that number to Web service Manager.

12) WSM get these information and create a format for these information plus information received from server and then forward to DigSig manager for digital signature.

13) DigSig Manager generate and send back that signature to WSM.

14) WSM create a proper format with information from step no 12 , digital signature of step 13 info and certificate of the android phone.

15) Step 14 encrypted information send back to Gateway of the web server.

16) Gateway receive that message, determine the identifier of the client using client certificate in message and sent the message to security manager.

17) Security manager sent back message after decryption to Gateway.

18) Gateway forward receiving digital signature of the client with public key to Digsig manager and also verifies random no of which is generated in step 6 that it is same??.

19) Digsig manager verifies the digital signature.

20) After successful verification of the android client, Gateway take the information unsigned from android client like random no of client, random number of the server which previously sent to client plus other message seq information forward to DigSig Manager for digital signature.

21) Then Gateway create message with unsigned part like random number of the server, message sequence, certificate of the server and digital signature forward to security manager and forward message to security manager for encryption.

22) Security manager encrypt that informations and send back to Gateway.

23) Gateway forward the message to android WSM.

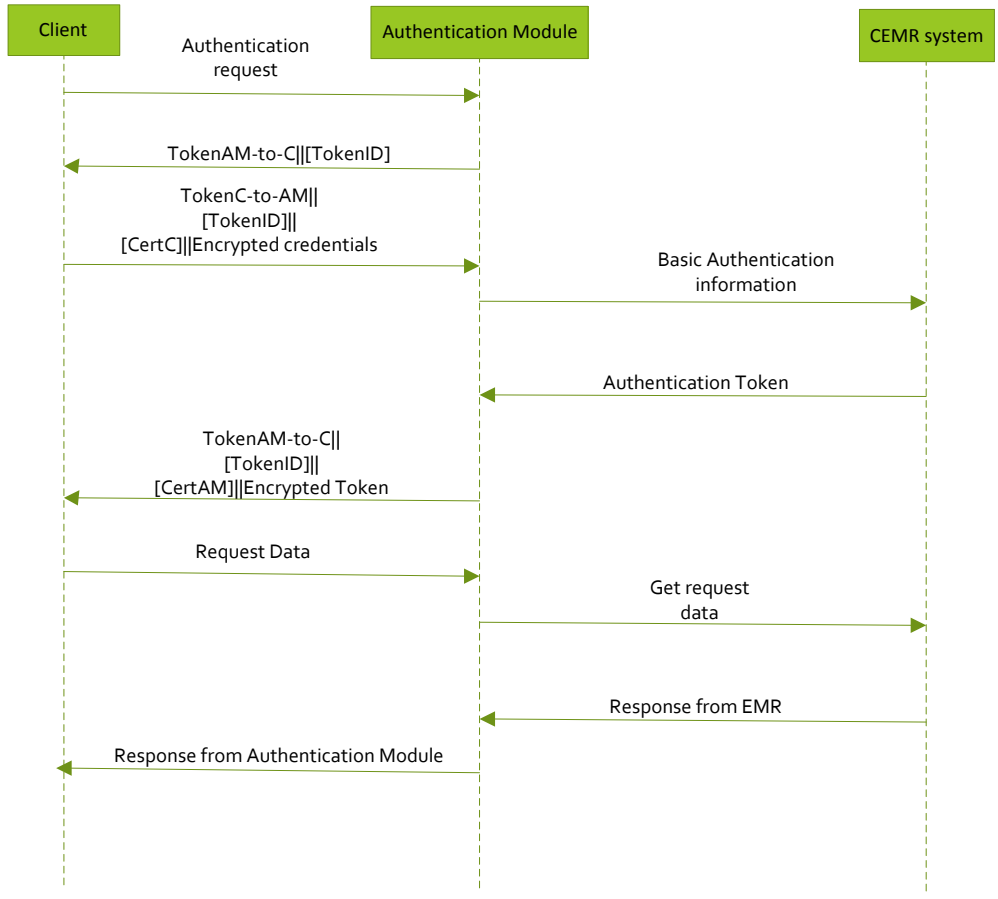
24) After receiving message, WSM forward digital signature for verification to Digsig manager.

25) If verification successful mean trust build.

26) Now actual credentials send to server by WSM with proper message format.
27) After decryption this message format send to gateway and after decrypting the message from security server forward to which actually create a basic authentication request for EMR system.
28) EMR system authenticate that user and generate a token for communication.
29) This token sent back with previous defined workflow to android client.
30) After that android client when need some resource it put token with previous way and sent to security manager on the Web server.
31) Security manager get that token and determine with the help of PDP (policy decision point) that requested resource can be permitted to this client or not.
32) It permitted then requested resource will be returned to client.
33) In case of rejection resource request will refuse by Gateway.

The sequence diagram for the authentication process shown below.

Figure 3.3 Sequence Diagram



Below are the description of abbreviation used in sequence diagram

- Client – C
- Authentication Module – AC
- EMR System EMRS
- Token AM-to-C means token from authentication module to client.
- Token C-to-AM means token from client to authentication module.
- Cert C means certificate of client.
- Cert AM means certificate of authentication module.
- [] optional fields.

- Token AM-to-C or Token C-to-AM include random number which is generated by C or AM plus some optional text.
- Token ID is sequence number during communication between C and AM.

Chapter 4

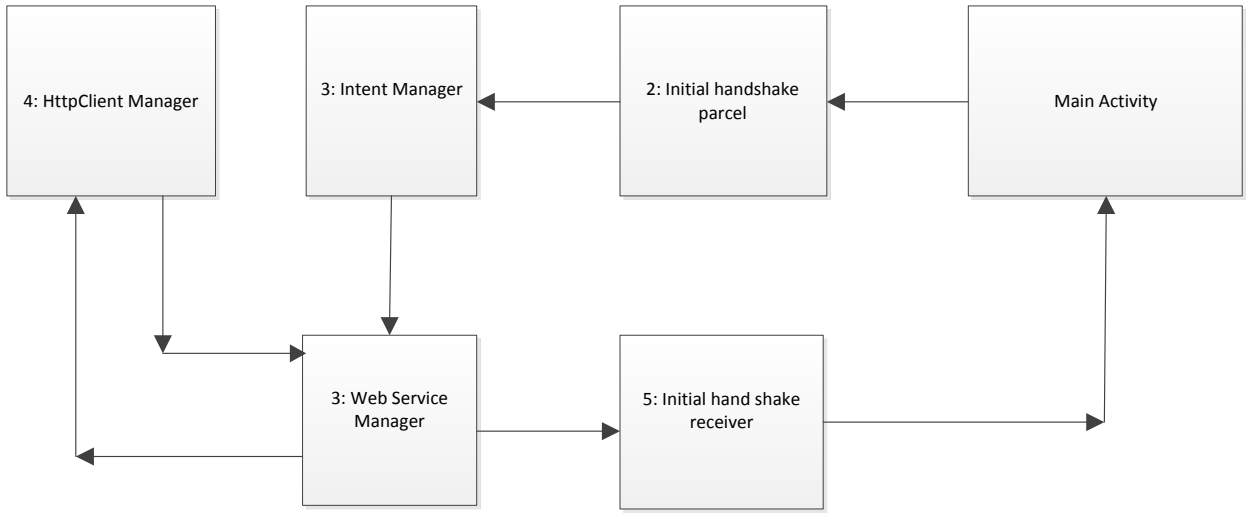
Implementation

This chapter discuss the implementation details of the system. It includes the several algorithms which are used for interaction between the components of the system and also some diagrammatic views of different components. Main components which interacting each other are Android client, Web server and EMR web server. So first we discuss implementation detail of android client application which is specifically implemented for our thesis problem solution. In implementation we throughout use on client side Android sdk, Java, JSON(for object name/value pair storage)

4.1 Android side implementation

First we discuss the android side implementation. A high level diagram shown below.

Figure 4.1



User interface loaded during startup. The android api use to create this user interface we call it main activity. Its basically exposes different functions like onCreate, onStart, onRestart etc to facilitate creation of user interaction controls. It is like a main process in android application. It remains in memory when call its onCreate method until call the onDestroy method. User interact with this and it pass user entered values to other components. Android allows us to use one activity at a time. So if we use simultaneously other activities with main activity. Then during other long time processing activities running main thread disturbed. For this reason we use the intent service which is working in background without disturbing the main thread. Below table show the Activity component various characteristics.

Table 4.1.1

Name of the component	Purpose	Package	Functions provide
ActionBarActivity	Interact with user Expose different function like onCreate, onStart, onRestart etc to facilitate creation of user interaction controls.	android.support.v7.app.ActionBarActivity	onCreate, onStart, onRestart onStop onDestroy etc

So when use background thread for long processing we need intent which actually launch a background service. The intent is basically a glue between different components of the system. It usually start other activities as well. It has two types of information action need to perform and data on which action will be performed.

Table 4.1.2

Name of the component	Purpose	Package	Attributes provide
Intent	Description of the function performed at abstract level.	android.content.intent	Action view Action edit Action main

As our architecture shows that android application calls the web services. So we need a platform where we can call the web service obtain a result and pass through the main activity. We use the intent service for this purpose. i.e call a web service, obtain a result and pass that result to main activity. To discuss intent service in detail first we describe the way we choose for getting user information from main activity. This purpose achieved through Parcel.

Table 4.1.3

Name of the component	Purpose	Package	Functions provide
Parcel	Messages container that will read or write.	android.os.Parcel	writeByte(byte) readString() etc

Another interface we use extensively in our implementation is parcelable. Parcelable is actually an interface which is implemented by those object which will be parceled.

Table 4.1.4

Name of the component	Purpose	Package	Functions provide
Parcelable	Classes implement this interface which instances later on write on to parcel or read from parcel.	android.os.Parcelable	writeToParcel describeContents.

Now we describe the intent service. Intent service is base class for service. Service can be visualize as a background facility which tells to parent application that some work is continuing in the background or communication with other applications. It usually perform the long time taken activities while its parent application do its tasks without any blockage.

Table 4.1.5

Name of the component	Purpose	Package	Function provide
IntentService	Base class for services, handle request on demand.	android.app.IntentService	onBind onCreate onDestroy

Result receiver is another interface which also work in our scenario. It gets data from intent service and update to main activity with desired data in name/value pairs.

Table 4.1.6

Name of the component	Purpose	Package	Function provide
ResultReceiver	Interface for provide callback data to main activity	android.os.ResultReceiver	Send writeToParcel

Along with these android core api we use our custom components for achieving our tasks. Web service manager is custom component which have purpose to manage calling web service, provide data to web server and then get output from web server and transform that output to our desire format. It also uses httpClient manager component for getting synchronous http clients. http client component is actually a client factory.

Table 4.1.7

Name of the component	Purpose	Package	Function provide
HttpClientFactory	For getting synchronous http clients	Nust.ms.thesis.finalthesis.factories	getThreadSafeClient

Web service manager calling web server. It tranforms the data into web server desired format and then after getting data from web server transform into android side desired format. Usually the data before calling the web service transform into JSON and then sends to web server. After getting result from web server in JSON format, it transforms into android client specific format. Below is its tabular description

Table 4.1.8

Name of the component	Purpose	Package	Function provide
webServiceManager	Manage calling web service, provide data to web server and then get output from web	Nust.ms.thesis.finalthesis.factories	getThreadSafeClient

	server and transform that output to our desire format		

RandGenManager used for random no generation.

Table 4.1.9

Name of the component	Purpose	Package	Function provide
randGenManager	Random no generation.	Nust.ms.thesis.finalthesis.randomgenerator	generateRandomNo

Digital signature manager used for digital signature generation/verification.

Table 4.1.10

Name of the component	Purpose	Package	Function provide
digSigManager	Digital signature generation and verification.	Nust.ms.thesis.finalthesis.digitalsignature	generateSignature verifySignature

4.2 Common library

The common library implemented because we need on android side and web server side same functionality. i.e messages formats are common between web server and android client side. This module implemented following

Communication between android and web server is in xml. Below the are the message formats.

Initially android app send message to start communication by simply sending its ip address to server. Then server respond to client initiate request with following response. The response include tokenId, server random no and some optional text. The message from server shown below in table 4.2.1

Table 4.2.1

Message from server Ist pass
< message message-owner = *"server"* > <tokenid token-type = *"0x0001" proto-version = "2" value = ""/>*

<message -from- server> <random-number owner = *"" value = ""* /> <text id = *"text1" value = ""* /> </message-from-server> < /message>

The client receive the response from server and then create response which includes its own tokenId, client random no, server random no which is being received from server, verifier entity name, some optional text and also with certificate of client.

Table 4.2.2

From android to web server message format
<message – from - client> <token-id token-type = "0x0002" proto-version = "2" value = ""/> <random-number owner = "server" value = "" /> <random-number owner = "client" value = "" /> <verifier-entity name = "ip address/ computer name" /> <text id = "text3" value = "" /> <certificate of client /> </message-from-client>

The server receive the response from client and then create response which includes its own tokenId, server random no, client random no which is being received from client, some optional text and also with certificate of server.

Table 4.2.2

From web server to android message format
<message – from - server> <token-id token-type = "0x0002" proto-version = "2" value = ""/> <random-number owner = "server" value = "" /> <random-number owner = "client" value = "" /> <verifier-entity name = "ip address/ computer name" /> <text id = "text3" value = "" /> <certificate of server /> </message-from-servert>

The client receive the response from server and then create response which includes its own tokenId, client random no, server random no which is being received from server, verifier

entity name, some optional text and also with authentication request information, in our case username password in encrypted form.

Table 4.2.3

Message from client
<message-from-clientt> <token-id token-type = "0x0002" proto-version = "2" value = ""/> <random-number owner = "server" value = "" /> <random-number owner = "client" value = "" /> <authentication result= “success/reject" value = "" > <ticket value = “” /> </authentication> <verifier-entity name = "ip address/ computer name" /> <text id = "text3" value = "" /> <data-signature> <random-number owner = "server" value = "" /> <random-number owner = "client" value = "" /> <verifier-entity name = "ip address/ computer name" /> <text id = "text2" value = "" /> ---subset of value text3 </data-signature> <certificate of the client> </message-from-client>

The server receive the response from client and then create response which includes authentication results success or reject. If authentication success then it gives the token value which will be used by client in subsequent calls.

Table 4.2.4

Message from server 2nd pass
<message-from-server> <authentication result= “”> <ticket value = “” /> </authentication> <resource id = “”> <response /> //will be in the form of xml </resource> </ message-from-server >

If client authenticated then it can get resource from web server. It pass certain parameters values to server for particular resource along with authentication token.

Table 4.2.5

Message from client 2nd pass
<message-from-client> <authentication result= “”> <ticket value = “” /> </authentication> <resource id = “” parameters = “comma separated”/> </message-from-client>

Above all messages formats implemented by common library. Below we discuss the implementation details. We use java api for xml binding. It automatically generates the JSON with simple using some annotations. TokenId contains the following information.

Table 4.2.6

Name : TokenID		
Attribute	Property Type	Description
tokenType	String	Unilateral/mutual authentication
protoVersion	String	Protocol version
Value	String	Actual token value

RandomNo contains the following information

Table 4.2.7

Name : RandomNo		
Attribute	Property Type	Description
owner	String	Owner of the random no.
value	String	Value of the random no.

Verifier entity is actually server ip address or name.

Table 4.2.8

Name : VerifierEntity		
Attribute	Property Type	Description
Name	String	Name of the verifier entity.

Message from server contains the following information

Table 4.2.9

Name : MessageFromServer		
Attribute	Property Type	Description
tokenId	TokenID	Token related information
randomNo	RandomNo	Random no related information
text	String	Name/value pair arbitrary information

Message from the client contains the following information.

Table 4.2.10

Name : MessageFromClient		
Attribute	Property Type	Description
tokenId	TokenID	Token related information
randomNo	RandomNo	Random no related information
verifierEntity	VerifierEntity	Verifier entity
text	String	Name/value pair arbitrary information

Final message after the whole authentication process completed.

Table 4.2.11

Name : FIPSMessenger		
Attribute	Property Type	Description
messageFromClient	MessageFromClient	Client message
messageFromServer	MessageFromServer	Server message
messageOwner	String	Owner of the message

4.3 Service Provider (Server side implementation)

We developed web services in java language using jersy web services and java api for xml binding (JAX-B). The service provider start working when android client call its service. First a servlet filter invoked. This filter typically designed for encryption/decryption tasks. i.e it decrypt the data when received through web service and encrypt when server response to a service call.

There are no of services for different purposes.

4.3.1 Login initiate service

The android client calls this service when it initiate the process of authentication. This service only receive client ip address. The server request for the random no generation to RandGenManager. RandGenManager generate no and pass this number to database manager for persisting this no to database and also return this no to service. The server make response as shown in table 4.2.2.

Table 4.3.1

Service name	Purpose	Input/output	Url
Initiate	Calling this service mean that client want to communicate with server	Json/json	Login/initiate

4.3.2 InitialResponseByClient service

This service accept the message which is shown in figure 4.2.3 then all values pass to DigSigManager for digital signature. The message format figure 4.2.4 return these values to client with accept or rejection of authentication information.

Table 4.3.2

Service name	Purpose	Input/output	Url
InitialResponseByClient	Client send its message after server first time respond	Json/json	Login/initialresponsebyclient

Client with authentication information calls below service. Service pass the authentication information to authenticator. The authenticator then pass these values to EMR system. If EMR system respond with token then authenticator return this token value to this service.

Table 4.3.3

Service name	Purpose	Input/output	Url
Authenticator	Calling this service mean that client sends its authentication information	Json/json	Login/authenticate

After successful completion of authentication process now client can request for a resource. It passes the token value along with resource description to server. This service passes this token to security manager. The security manager then check that this client can request for this resource i.e authorization. If it is authorized for this resource then below service call the openMRS web server for this particular resource. After getting response from openMRS server it returns response to client.

Table 4.3.4

Service name	Purpose	Input/output	Url
resourceRequest	Calling this service mean that client request for a particular request	Json/json	Login/resource

Chapter 5

Conclusion

With the advent of virtualization, high speed availability of internet and distributed computing techniques make computing resources cheaper, more dominant and more available than ever. Most of the world business shift from traditional IT systems to new computing model in recent years and this new computing model is called cloud computing. The new model offers new features to healthcare domain to enhance their functionality. So this domain is shifting rapidly from traditional computing to cloud computing. In healthcare domain different stakeholders like physicians, insurance companies, patients, healthcare providers need to work together. For information processing/sharing among different stakeholders cloud computing is best option in terms of cost, time, throughput and service uptime. Shifting from traditional EMR system to cloud implies that there are several threats in terms of security and privacy. This is main barrier because of which healthcare industry feel hesitation to transform its services on cloud.

In our research we propose a secure architecture for the EMR. Authentication service implemented using extended FIPS 196 authentication protocol. i.e before exchanging sensitive information on cloud between client and server, must exchange random numbers and generate/verify digital signatures. Once authenticated a user, then at every call checked that user has required permissions to access a resource on EMR or not. For this purpose specific policy decision point implemented that decides access or rejection for that particular resource on EMR.

5.1 Future Work

It is first step towards healthcare privacy implemented on existing system. Now a days more and more companies shifted from traditional EMR systems to cloud based EMR. For newly cloud based EMR implementations, with minor changes in our implemented system, it can be used as a separate authentication and authorization system.

References

1) Fan, L.; Buchanan, W.; Thummler, C.; Lo, O.; Khedim, A.; Uthmani, O.; Lawson, A.; Bell, D. DACAR Platform for eHealth Services Cloud. In *Proceedings of the 4th International Conference on Cloud Computing*, Miami, FL, USA, July 2011; pp. 219–226.

2) Integrating the Healthcare Enterprise Online. Available: http://ihe.net/

3) AbuKhousa E, Mohamed N; Al-Jaroodi J; e-Health Cloud: Opportunities and Challenges , July 2012

4) Doukas, C. ; Samos, Greece ; Pliakas, Thomas ; Maglogiannis, I.Mobile Healthcare Information Management utilizing Cloud Computing and Android OS, Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Dec 2010;

5) Sanjay P. Ahuja, Sindhu Mani, Jesus Zambrano. A Survey of the State of Cloud Computing in Healthcare, Canadian Center of Science and Education, Sept 2012, Vol. 1, No. 2;

6) J Hu, AC Weaver, A Dynamic Context-Aware Security Infrastructure for Distributed Healthcare Applications, Online. Available: http://www.cs.virginia.edu/~acw/security/doc/Publications/A%20Dynamic,%20Context-Aware%20Security%20Infrastructure%20for%20Distri~1.pdf

7) Angin, P.Bhargava, B. ; Ranchal, R. ; Singh, N. ; Linderman, M. ; Othmane, L.B. ; Lilien, L. An Entity-centric Approach for Privacy and Identity Management in Cloud Computing; 29th IEEE Symposium on Reliable Distributed Systems, Nov 2010

8) Richard Chow, Markus Jakobsson, Ryusuke Masuoka, Authentication in the Clouds: A Framework and its Application to Mobile Users; CCSW'10, Illinois, Oct 2010

9) O'Gorman, L. ; Basking Ridge; USA Comparing Passwords, Tokens, and Biometrics for User Authentication; Proceedings of the IEEE (Volume:91 , Issue: 12), Nov 2004 pp 2021-2040

10) Bhutta, F.K. Ghafoor, A. ; Sultan, S. Smart phone based authentication and authorization protocol for SPACS. 9th International Conference on HONET, Istanbul, Dec 2012; pp 127-131

11) Alex Mu-Hsing Kuo (2011, Sept 21) Opportunities and Challenges of Cloud Computing to Improve Health Care Services, Online. Available : http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/

12) Grindle M, Kavathekar J, Wan D; (2013) A new era for the healthcare industry Online. Available: http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-New-Era-Healthcare-Industry-Cloud-Computing-Changes-Game.pdf

13) Health Insurance Portability and Accountability Act (HIPPA) of 1996, Pub.L. 104–191, 1996.

14) Singh R K, Bhattacharjya A; Security and Privacy Concerns in Cloud Computing, International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 6, June 2012

15) Yuan E, Tong J; Attributed Based Access Control (ABAC) for Web Services, Proceedings of the IEEE International Conference on Web Services, Virginia, 2005

16) Shakeeba S. Khan *et al*, Security in Cloud Computing Using Cryptographic Algorithms, International Journal of Computer Science and Mobile Computing, Vol.3 Issue.9, September- 2014, pg. 517-525

17) Itani, W.Kayssi, A. ; Chehab, A. Autonomic and Secure Computing, Eighth IEEE International Conference on Dependable, Dec 2009. Chengdu, pg 711 – 716

18) Botts, N. ; Thoms, B. ; Noamani, A. ; Horan, Thomas A. Cloud Computing Architectures for the Underserved: Public Health Cyberinfrastructures through a Network of HealthATMs, 43rd Hawaii International Conference on System Sciences (HICSS) Honolulu HI, Jan 2010, pg 1 – 10

19) Rolim, Florianopolis, Koch, F.L.; Westphall, C.B. ; Werner, A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions, Second International Conference on eHealth, Telemedicine, and Social Medicine, St. Maarten, Feb. 2010, pp 95 - 99