5.1 INTRODUCTION

Cloud computing is a service on demand i.e. pay and use service. It offers subscription-based access to infrastructure, platforms, and applications that are popularly known as IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and SaaS (Software as a Service). These emerging services have increased interoperability, usability, reduced the computation cost, hosting of application, content storage and delivery by several orders of magnitude.

Currently maintenance of patient’s medical records and reports are through centralized system without sharing facility with other health centres as shown in figure. There is no freedom to the patients to obtain their medical information like treatments, reports via mobile devices.

Figure 5.1 Existing Healthcare systems
The gifted application area of cloud computing is keeping patient’s healthcare and their medical reports on cloud ecosystem. The mobile cloud ecosystem for patient’s healthcare has lots of advantages. Some advantage of this cloud ecosystem is storing patient’s information in cloud database with synchronization. The information is integrated and shared among different medical departments, institutions, hospitals and other public and private health centres. This system will provide freedom of the patient to go under medical check-ups and treatments from their nearby health centre under the supervision of expert doctors located remotely regardless of their physical availability. Use of mobile devices with cloud environment sustain interaction among different healthcare cloud would enable the patients to get the better health service. Experimental results demonstrate fine performance in comparison with conventional systems.

Cloud computing presents unusual risks like security and confidentiality of patient information, interoperability, fulfilment with government regulation and network security. So it is very important to understand the value of addressing these risks in healthcare organizations and taking into consideration that cloud computing need to carefully consider the risks before it take place. A Randomized Alphanumeric Cipher (RAC) algorithm introduced to secure the patient information and enhancing the confidentiality and also to ensure the privacy of users.

5.2 HEALTHCARE CLOUD ECOSYSTEM

Virtualization has revolutionized centre of data technology with the help of a set of techniques and tools that facilitate the provision and management of the dynamic data centre’s infrastructure. It has become an essential and enabling technology of mobile cloud computing environments. Virtualization can be defined as the abstraction of the four computing resources is storage, processing power, memory, and network or I/O. It enables high, reliable, providing on-demand service and lives migration services which improve reliability with real time. Accordingly, an effective management suite for managing virtual machines infrastructure for any mobile cloud computing infrastructure as a service (IaaS) vendor.
A model is proposed for storing patient’s information and medical reports in secured synchronized mobile cloud ecosystem which provides facilities to the patients to go under medical treatments at any time. As the system is digital and available over the mobile network no need of hard copy of their medical reports. Wherever they move for health concern, since these medical reports are their own life sustainable documents they can access these whenever they need as it is service on demand through mobile devices.

![Figure 5.2: JXTA Healthcare Cloud Ecosystem](image)

As mobile cloud computing is achieving increased popularity, concerns are being expressed about the security issues introduced through had option of new models. The effectiveness and efficiency of traditional protection mechanisms are being
reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of applied security and that similar security principles that apply in shared multi-user mainframe security models apply with mobile cloud security. Here cloud made up of computers is extending beyond a single company or an enterprise.

5.3 WORKING MECHANISM

A model is proposed for keeping Patient’s Health records in secure and synchronized cloud environment which provides the facilities to the patients to get their health information anytime anywhere. As the system is digital and available over the network i.e. internet patients don’t have to worry about carrying a hard copy of their original documents wherever they move, since these documents are their own personal health assets they can access these whenever they need it that is service on demand. For a patient who migrates from one place to another where all his records are kept separately to the hospitals respectively and considered as different Hospital clouds. As cloud computing is achieving increased popularity, concerns are being expressed about the security issues introduced through adoption of new models. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model can differ widely from those of traditional architectures. An alternative perspective on the topic of cloud security is that this is but another, although quite broad, case of applied security and that similar security principles that apply in shared multi-user mainframe security models apply with cloud security. Here cloud made up of computers is extending beyond a single company or an enterprise. The applications and data served by the cloud are available to broad concerned group of users; it crosses enterprise and crossed the platform.

In the proposed model we build a cloud ecosystem in which all the concerned patient data clouds and the hospital clouds will be synchronized and will communicate with each other based on the insolvent of student’s identity. We will provide strong authentication and security ID to the student to log into the cloud ecosystem and to get their patients records anytime anywhere patient’s
are pursuing their datas in different hospitals and Health professionals. Here cloud made up of computers is extending beyond a single hospital. The applications and data served by the cloud are available to broad concerned group of users that is student; Service is accessed via the Internet. Any authorized patient can access these docs from any computer over any Internet connection. And, to the user, the technology and infrastructure behind the cloud is invisible. The applications and data served by the cloud are available to broad concerned group of users. Service is accessed via the Internet. It is apparent in most cases the cloud services are based on HTTP, HTML, and XML, JavaScript, PHP or other specific technologies.

A secure mobile cloud ecosystem is present in which all the concerned healthcare clouds would be synchronized and would communicate with each other based on the insolvent of patients identity along with doctor’s ID. To make systems available to patients and the concerned doctors on mobile, we used. We provide authentication and security with the help of Randomized Alphanumeric Cipher (RAC) algorithm. The patients will log into the mobile cloud ecosystem and to get their medical information and prescription anytime anywhere. This network let peers send and receive messages (these messages are being encrypted and decrypted with RAC algorithm) from each other, independently from its network location.
Figure 5.3: Randomized Alphanumeric Cipher (RAC) algorithm
5.3.1 ENCRYPTION ALGORITHM

1. We are generating N number of 8 bit alphanumeric characters randomly
2. Random Selection one in that which is represented as ‘A’, a 5-bit SECRET KEY assigned as ‘B’.
3. Binary format of A and b are converted
4. Z=A/B the quotient is evaluated
5. XOR operation is performed with Message ‘M’ and quotient ‘Q’, TEXT = M XOR Q.

5.3.2 DECRYPTION ALGORITHM

1. Extra bit is removed from CIPHERTEXT.
2. XOR operation is done with ‘TEXT’ and quotient ‘Q’.
3. Message M is obtained.

5.4 ILLUSTRATION

Table 5.1 Hospital Data’s stored

<table>
<thead>
<tr>
<th>S.No</th>
<th>Hospital ID</th>
<th>Doctor ID</th>
<th>Patient ID</th>
<th>Document Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4KMP33</td>
<td>LP6</td>
<td>13BL49</td>
<td>13BL49.docx</td>
</tr>
<tr>
<td>2</td>
<td>7DNS45</td>
<td>SK8</td>
<td>12CH59</td>
<td>12CH59.avi</td>
</tr>
<tr>
<td>3</td>
<td>8CMQ39</td>
<td>SR5</td>
<td>11MS43</td>
<td>11MS43.doc</td>
</tr>
<tr>
<td>4</td>
<td>7KLS41</td>
<td>KM2</td>
<td>65SD83</td>
<td>65SD83.docx</td>
</tr>
<tr>
<td>5</td>
<td>8STP25</td>
<td>GM6</td>
<td>63SP48</td>
<td>63SP48.mpeg</td>
</tr>
</tbody>
</table>

Table 5.2 Patient ID obtained after Encryption and Decryption

<table>
<thead>
<tr>
<th>S.No</th>
<th>Patient ID</th>
<th>Patient ID Obtained</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>13BL49</td>
<td>0011000100110000100000011010000111001</td>
</tr>
<tr>
<td>2</td>
<td>12CH59</td>
<td>001100010011000011010000011100100001</td>
</tr>
<tr>
<td>3</td>
<td>11MS43</td>
<td>001100010011000000110100000011110000001</td>
</tr>
<tr>
<td>4</td>
<td>65SD83</td>
<td>001100010011000010001000011100000001</td>
</tr>
<tr>
<td>5</td>
<td>63SP48</td>
<td>001100010011000011000100001100000001</td>
</tr>
</tbody>
</table>

59
5.4.1 SAMPLE ENCRYPTION AND DECRYPTION OF PATIENT DATA

1. Public key (Hospital ID) = 8CMQ39
Binary equivalents [8= 00111000, C= 01000011, M= 01001101, Q= 01010001, 3= 00110011, 9= 00111001]
Concatenating 8CMQ39=00111000 01000011 01001101 01010001 00110011 00111001

2. Secret key (Doctor ID) = SR5
Binary equivalents [S= 01010011, R= 01010010, 5= 00110101]
ConcatenatingSR5= 01010011 01010010 00110101

3. Message (Patient ID)=11MS43
Binary equivalents [1=00110001, 1=00110001, M=01001101, S= 01010011, 4=00110100, 3=00110011]
Concatenating11MS43=00110001 00110001 01001101 01010011 01010010 00110011

4. Quotient ‘Q’; Q=(Public Key)/(Secret Key)=(Hospital ID)/(Doctor ID)

\[
(00111000010000110100111010100010011001101111001) / (010100110101001000110101) = 101011001101110101101101101111011011110111011011111011110111011011
\]
(We have truncated the values right side of decimal part) then it become
Q=10101100110111001101101

5. XOR operation with Message (Patient ID) and Quotient Q
=> Ciphertext1=(Patient ID)XOR(Quotient Q)
\[
(001100010000101001101010010100010011001101111001) XOR (1010110011011101011011011111011011110111011011111011110111011011) = (00 11 00 01 00 11 00 01 01 00 11 01 01 01 00 11 00 11 01 00 00 11 00 11) XOR (00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 10 11 00 11 01 11 01 01 10 11 01)
\]

60
(We have added zeros 0 to left side of Quotient for equality of both since it does not affect the operation)

Ciphertext1=(00 11 00 01 00 11 00 01 01 00 11 01 11 11 11 11 11 11 10 10 01 01 01 11 10)

First level of encryption due to XOR operation.

5. Now whole Ciphertext1 is scanned from left to right for checking the pattern as specified in flowchart.

\[
00110001001100010100110111111111111110100101011110 \\
(111 sequences found 5 times)
\]

7. Cipher text 2=Ciphertext 1 with Bit-stuffing and stuffing using SECRET KEY case 1 as per flowchart since it follows 111 combination of sequence. We took bits from right hand side of secret key for bit stuffing. Secret Key bits which are not used have been concatenated at last.

Cipher text 2 = Secret Key bits = 01010011 01010010 001 1010111101010010 001 1001000100110101010010 001

(111 sequences found 5 times)

It was second level encryption. Thus we got encrypted form of patient Id similarly we encrypted all information of the patient.

5.4.2 DECRIPTION OF PATIENT DATA

It is the reverse of encryption.

Input

Ciphertext2=0011000100110001010011011111111111101001011111111001001
01010001001101010011010010 001
01010011 01010010 001

1. Remove Concatenated bits from cipher text 2.

\[
001100010011000101001101111111111110100101111111111001001 \\
01010001001101010011010010 001 \\
01010011 01010010 001
\]

Removed bits=01010011 01010010 001

2. Remove each fourth bit followed by the occurrence of triple one (111) sequence. And append these bits at the end of previously removed bits.

3. If these removed bits are equal and same as secret key the left sequence will become cipher text 1 as it is.
4. Ciphertext1 XOR quotient Q will result us original message we mean the patient ID

\[(00110001001100010100110111111101010111001011011101)\]

\[\text{XOR}\]

\[(0000000000000000001010101100110110110101101101011010000110011)\]

Now by separating 8 bits group from left to right we got patient ID 11MS43 = 00110001 00110001 01001101 01010011 00110100 00110011

5.5 IMPLEMENTATION OF HOSPITAL CLOUD ECOSSTEM

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

5.5.1 CLIENT MODULE

In the client module client need a web browser to send query to the server. Based on the requested query the server sends the corresponding file to the client. Before this process, the client authorization step is involved. In the server side, it checks the client ID and its password for security process. If ID and password is matched then it processes the queries from the client and searches the corresponding files in the database. Finally as response server sends requested data to the client.

5.5.2 SYSTEM MODULE

- Creating Cloud Container
- Downloading RSA private access key
- Testing Connectivity
- Database Configuration
- Drag and Drop apps to Container
5.6 CREATING CLOUD CONTAINER

A container is a small version of the Zend Application Fabric. The Fabric is a standardized system of runtimes, components and APIs based around Zend Server. It is the most general feature and most other features will be housed within the container. It contains an instance of Zend Server, who’s UI (User Interface) we can access from within that container’s UI via a button on the top.

![Image of container creation interface](image)

Figure 5.4 (i) Container (ii) Deployed Application

This container also contains our MySQL instance and any applications that need to access that application. Each individual application in our container will need to share that database. If you need to have applications segmented from each other then we will need to either create an additional container...
which will use the standard MySQL extensions. All applications are housed within a container on Zend Server. This container is separate from all other containers and has its own database instance and is easily connected to our IDE. We can easily get started by publishing your application to Zend Developer Cloud container or by starting with one of the pre-packaged applications and integrating them into your local IDE or by pushing your existing project to one of your containers using Zend Server's deployment mechanism.

5.7 DOWNLOADING RSA PRIVATE ACCESS KEY

zendcloud-v7n_2jab2k3g8v0fe656.pem

PEM Files are the standard format for Open SSL and many other SSL tools. This format is designed to be safe for inclusion in ASCII or even rich-text documents. A single PEM file can contain a number of certificates and a key, for example, a single file with:

- Public certificate
- Intermediate Certificate
- Root certificate
- Private key

The PEM file type is primarily associated with 'Privacy Enhanced Mail Security Certificate'. In cryptography, a public key certificate (or identity certificate) is a certificate which uses a digital signature to bind together a public key with an identity. The certificate can be used to verify that a public key belongs to an individual. These can be a personal certificate or a Certificate Authority certificate.

5.7.1 TESTING CONNECTIVITY

In order to testing the connectivity with Zend studio IDE, we have to create local phpproject followed by deployment mode, we select the phpcloud as deployment mode after clicking next tab popup window will ask for username, password and SSH private key as shown in below figure:-

64
We have to provide Username as container name which is created in phpcloud.com and password is container password, for SSH private key we have to give the path of “zendcloud-v7n_2jab2k3g8v0fe656.pem” which we have downloaded during container creation. After all we click on finish button, hence it will consume some moment for test connection.

We can manage our database instance using provided phpMyAdmin interface, which we can access in our application container control panel, under the "Management" tab.

5.8 SNAPSHOTs

All the Patients registered in the mobile cloud ecosystem among these, according to 100 patient disease symptoms they were referred to the general physician, new users can also register in this cloud.
Patients registered to the system with require fields like patient ID, doctor ID and date of birth.

Patient login to the system by filling patient ID and password in the cloud.
Patient views his/her health profiles anywhere anytime through his login from the cloud.

Patient view the doctor details and easily consult them.
5.9 CONCLUSION

This system was developed for mobile healthcare cloud applications and is designed to support the mobile healthcare cloud ecosystem. The simulated results show that this system can bring freedom and mobility to the patients to go under treatment with proper supervision in a secure way. Controlling and monitoring by the doctor makes the system more flexible and structured. Enhanced studies are needed to improve the system as compared with the traditional system.