International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

Secure Web Based Health Care System Using Homomorphic Encryption

Dr. Preeti Patil[1], Shubham Davate[2],Rishikesh Jagtap[3],Rishikesh Devkate[4],Apoorv Gajbhe[5]
[1]*Head Of Department Of Information Technology, DY Patil College Of Engineering, Akurdi*
[2,3,4,5]*Student , Department Of Information Technology, DYPCOE Akurdi*

Abstract- In today's world most of the organizations prefers online storage of their data rather than physical storage. As online storage have certain advantages over traditional physical data storage such as on demand service, cost effective, reliable and scalable service. But with certain advantages there is one big issue related to online storage is of security of data stored on online platform. To provide security various cryptographic algorithms are proposed and used but these traditional algorithms are not reliable in today's attacker era. So in this article we provide best way to secure Patients medical records using homomorphic encryption scheme. Due to fast growing life-style, Nobody gives time health related problems. Every person on this earth lives with certain kind of lifestyle irrespective of health concern. Whenever we visit hospital for minor health related problems and then later ignore precautions and treatment cause. So by using our proposed system Patient can keep his/her previous medical history in a database and this database is will keep on cloud platform by applying homomorphic encryption technique so that no one except that Patient can see his/her medical records.

1. INTRODUCTION

Due to advancement in technology and cloud computing it becomes easier for organizations to organize their huge data on cloud platform. Cloud provider provides on reliable and on demand service and also one can access his/her data from anywhere by using any device. But security is again the main concern of online data storage system. As cloud provider provides firewall and other such external security to cloud but data which is on third party/cloud is in open format. So to overcome this drawback of cloud security many different public key and private key algorithms are produced. These algorithms provides security to certain level but in today's modern quantum world these algorithms are not that much reliable as new age modern computers can easily decipher the message which is encrypted using traditional cryptographic algorithms. So to provide more reliable solution to these problem modern cryptography joined the field of security and provide homomorphic encryption techniques to securely stored data on cloud. By using homomorphic encryption techniques we can securely stored our data on third party/cloud. So we can extends this scope to secure Patients and Doctors databases which contains medical records of patients stored on cloud. Due to this two objectives are covered that is we can provide online system to stored medical records so that there is no need to carry papers and files and we can stored these records on cloud using homomorphic encryption system. we can use this for more confidential and trust worthy transfer services like to maintain medical databases and to use paperless medical science field with fully homomorphism. Additionally record is maintained with double encrypted on this hub hard party without giving access to server so that avoids Man in Middle Attacks. If it can be used widely then it can be act as a professional platform to connect patient and doctor in medical science field. When homomorphism has been applied on encrypted data old data get lost automatically which is stored on third party.

2. LITERATURE SURVEY AND EXISTING WORK

Information security is an growing issue in today's quantum world as most of the organizations keeps their data on cloud and attackers find new and innovative way to hack and bypass any cloud firewall using new age quantum computers. Traditional security algorithms are vulnerable to security attacks. So to overcome such problem security algorithms like AES, DES and RSA are produce. But these cryptographic algorithms are gets easily hacked and data is available to attacker easily.

Because of such drawback of traditional cryptosystems Modern cryptography joined the field to provide more reliable and efficient solutions to securely stored data on cloud. Modern cryptographic system contains concepts such as partial homomorphism and fully homomorphism. In modern cryptography mainly Partial homomorphism is the technique used to provide security to the cloud data. Homomorphism concept provides encryption on already encrypted data so that data stored on online platform should be in double encrypted format and it is extremely difficult for the attackers to retrieve original message from doubly encrypted data on cloud. So the now a day's organizations uses Partial homomorphism to secured data. In Christian A. Reuter's article [1] "A Guide to Fully Homomorphism Encryption", author represented the idea and concept of fully homomorphic encryption and give description on how this encryption works. In fully homomorphism author extend the scope of mathematical function 'f' to any mathematical operation and used any mathematical operation on already encrypted data to provide double encryption. Due to this we can used any mathematical operation and combination of mathematical operations such as simultaneous multiplicative and additive operation to perform operation on encrypted data to double encrypt that data and stored on cloud. Also author gives the idea of function encryption and obsfunction.The drawback of this system is that the algorithm given is inefficient due large overhead produced by mathematical operations.

In Yasmina Bensitel and Rahal Romadi's article, [3] "Secure data storage in the cloud with homomorphic Encryption" authors represent the concept and algorithm of Partial homomorphism. In partial homomorphism they used either used additive or multiplicative operations to stored data. Author used RSA algorithm for multiplicative partial homomorphism and also described the concept of "Somewhat Homomorphic Encryption". The problem with this system is that they use of Partial Homomorphic Encryption which is less secured as compared to Fully Homomorphic Encryption and also Keys which are used for encrypting and decrypting cipher text are not secured and keys are stored as it is on cloud's database.

3. TRADITIONAL AND MODERN CRYPTOGRPHY

3.1Traditional cryptography

The field of cryptography is primarily divided into two main categories and they are 1] Symmetric Cryptosystem and 2] Asymmetric Cryptosystem. Symmetric cryptography uses similar key to encrypt and decrypt the data/message. But if intruder/attacker recogniethe pattern of repeated words or somehow find the key then attacker can easily hack the data and decrypt it or attacker can make thewhole message passing and data storing system vulnerable. So to overcome this drawback of Symmetric Cryptosystem Asymmetric Cryptosystem comes into practice which uses pair of keys in which one key is called as public key used for encryption of message and another key called as private key used for decryption of encrypted data. This Asymmetric key cryptography is used more widely than Symmetric key cryptosystem as it is more reliable and secured than Symmetric key cryptosystem. Dueto its two keys it is extremely difficult for attacker and intruder to decipher the message even if he gets public key. Based on this some algorithms are produced to provide security to data using symmetric and asymmetric cryptosystem.

3.1.1 *Data Encryption Standard(DES)* :

Data Encryption Standard(DES) is an symmetric key cryptographic algorithm whichuses block cipher method. It takes 64-bit plaintext as an input and creates 64-bit ciphertext and data is encrypted using 56-bit key. DES performs various operations like Initial permutation, P-box and S-box permutation and final permutation to encrypt and decrpt the data. There are two moretypesof permutations used for more security purpose and they are DOUBLE DESand TRIPLE DES. But DES algorithm is vulnerable to Brute force attack and Meet-in-middle attack.

3.1.2 *Advanced Encryption Standard(AES):*

Advanced Encryption Standard(AES) is also symmetric key cryptosystem as DES but AES encrypts plaintext in 128,192 and 256 bits size and convert into ciphertext of similar size. Also, key size of AES is vary with respect to plaintextsize as 128,192 and 256 bits key. AES uses methods like SubBytes,ShiftRows,MixColoumns and

AddRoundKey to encrypt the data and perform reverseordering of these rounds to decrypt the data and get original message.

***3.1.3** RSA Algorithm:*

RSA is an Asymmetric key means public key cryptosystem algorithm which uses two separate keys to encrypt and decrypt the messages. RSA is developed by Rivest, Shamir and Aldeman and it is an block cipher algorithm. The security of RSA is depends upon complexity of two prime numbers and value of 'e'. RSA is known as first algorithm with homomorphic properties[7].

However, this algorithms are not reliable in modern world as their complexity is depends upon prime numbers and their compuation and attacker can easily get theseprime numbers using quantum computers and new techniques whichsuperfastly processed and find the prime numbers used for encryption process and thus attacker can able to decrypt the information easily[4].

3.2 ***Modern cryptography***

As traditional cryptosystems are inefficient for data security so that modern cryptography joined the field of cryptography to provide more efficient and reliable solution to securely store data on global server. Modern cryptography uses two popular and most effective techniques known as partial homomorphism and fully homomorphism. These techniques are dealing with more complex and deeper mathematical operations so that even if attacker bypass the firewall of cloud he never gets original data and it creates difficulty for attacker to get original message/data.

***3.2.1** Partial homomorphism:*

Homomorphism is the technique in which encryption is applied on already encrypted data so that data appears in the double encrypted format. Partial homomorphism is the technique which applies either additive or multiplicative operation on already encrypted data. In partial homomorphism scope of mathematical operation is limited as it uses either additive or multiplicative operation. RSA is the first algorithm having a homomorphic property and it uses Additive homomorphism to doubly encrypt data. Paillier's cryptosystem is another cryptographic system which possesses homomorphic property and follow multiplicative homomorphism[6].

***3.2.2** Fully homomorphism*

Fully homomorphism is an advancement in partial homomorphic scheme as in fully homomorphism we can extend the scope of mathematical function to any mathematical operation. Fully Homomorphic Encryption is termed as revolution in the field of cryptography which extends the scope of computations and perform operations on already encrypted data. Fully homomorphic encryption (FHE) is also called as the holy grail of cryptography, used to solve IT related problem regarding trust and security. That is fully homomorphism allows arbitrary computations on encrypted data. So in fully homomorphism we can perform additive as well as multiplicative operations on data simultaneously. In partial Homomorphism Scheme user cannot operate on the data and must download the data to perform the computations locally, with fully homomorphic encryption the cloud can perform computations on behalf of the user and return only the encrypted result[5][6].

4. SYSTEM ANALYSIS AND PROPOSED ARCHITECTURE

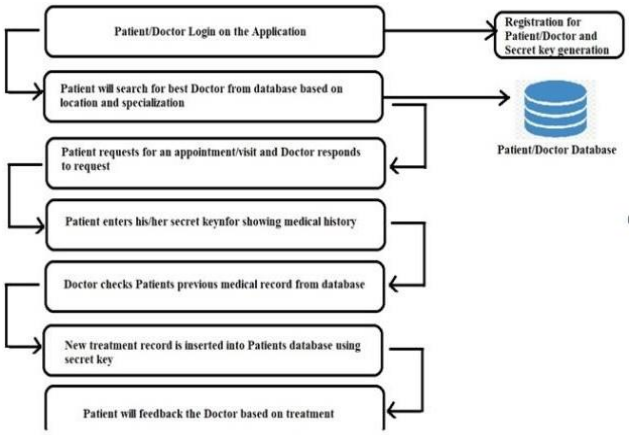
Currently existing system to provide security to online stored data is using partial homomorphic encryption. But this partial homomorphism allows only one type of homomorphic operation that is additive or multiplicative. So partial homomorphism provides more secured environment to store data on cloud as compare to traditional cryptographic systems but it is inefficient as compare to fully homomorphism. Due to this Partial Homomorphism is not that much reliable and inefficient so we proposed algorithm and system for Fully Homomorphism as fully homomorphism allows us to perform simultaneous additive and multiplicative operation as well as extend the scope of mathematical function to any mathematical operation. That's why we extend the concept and scope of Fully Homomorphism in the field of Medical Science to securely stored Health related data on cloud. In existing system Patient needs to carry his/her previous treatment records with them in traditional file system and it creates lots of problem when such file gets lost. By considering this disadvantages of traditional file system we proposed

an online application system in which Patient can easily stored his medical records and prescriptions. Due to such application there is no need to carry file or papers when Patient visits Doctor for his medical checkup. Also, we provide facility for Patient to search for best Doctor based on location, specialization and by checking reviews of any Doctor. In this system we keep Patients health related sensitive data on cloud as well as we keep feedback system for doctor as patient gives reviews to doctor as per treatment. Existing system does not provide any security to the keys which are used for encryption and decryption when such keys are keeping on cloud. So in our approach we applied encryption to keys as well so that keys are also stored securely on cloud in separate database. In this application we provide double encryption to Patients database as well as Doctors database. So by this we can securely stored Patients database on cloud and also Doctors database related to Review System is also stored securely in double encrypted form on cloud. And in our system Patients database is updated and altered by Doctor, only when Patient provide his secret key to decrypt that double encryption. And Patient can give review to Doctor when Doctor provides his secret key to decrypt the double encryption.

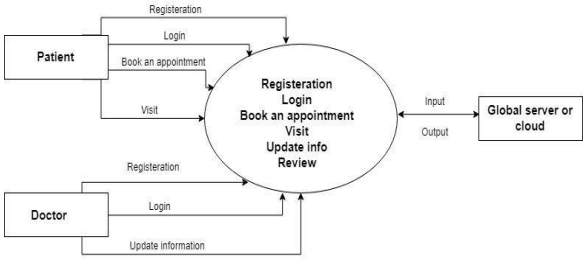
To stores health related data on cloud three databases are required to stored data related to Doctor, Patient and Keys.Doctor's database is used to stored Doctor's review related information and registration data which is also stored with homomorphism encryption and only Patient can give review to Doctor based on treatment of that Doctor, so that it will be beneficiary for Patient to find Best Doctor based on Specialization, Location and Review.

Patient's database is used to stores the data related to Patient's sensitive health related information along with Patient's registration information and these data is stored with homomorphism so that third party cannot access original data and only patient has right to access his/her information. Third database is related to Keys which are used for decryption of homomorphism encryption. In our system we are also providing protection to Keys by using double encryption and stored these Keys on global database in doubly encrypted format.

4.1 PROPOSED SYSTEM

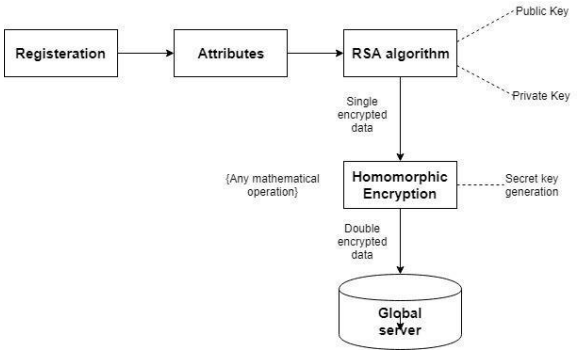


Above figure demonstrate the system design and architectural view of how this application will work. Our system represents the idea for medical science and for involving it into all over world as government based activity. Because it will effect on every person's health. When any Patient wants first time medical health checkup he/she has to register online on this application. Then based on attributes he filled during registration will used to generate one PID number for everyone those who will register. So, when he or she wants to consult himself/herself, it is compulsory for them to enter PID for logging into the application. Then Patient can use his/her location details and type of specialized Doctor he/she wants to consults to find best Doctor based on following attributes as well as by checking reviews of that particular Doctor. When Patients information is on cloud it creates one Secret Key which is used when Patient physically visits any Doctor with prior appointment to show that Doctor his/her previous medical records. Doctor will treat Patient by checking his/her previous medical records and update/insert new records based on current treatment. Patients records are only altered by Doctor when Patient provides his/her Secret Key and decrypt its health related records. Also, we provide review/feedback/rating policy in which Patient can give reviews to Doctor based on Doctor's treatment when Doctor provides his/her Secret Key during physical visit.



It is the part of system analysis. In this we show that how the data is flow. Here we show that how Patient and Doctor perform various processes on Web applications and how Global Server is used to stores double encrypted data as well as how by using Secret Key we can retrieve original data.

5. ALGORITHM AND MATHEMATICAL MODEL



1. When Doctor and Patient registered themselves on web server they are free to set their own password
2. Consider password entered by Patient/Doctor during registration as one attribute and with respect to this attribute set the value of variable 'e' to perform RSA operation on data for that particular user.

5.1 RSA Algorithm:

a) First, we have set of random prime values at backend in the database say p= {11, 17, 23, 29, 47}

b) Create random p and q prime numbers selected from stored database.

c) For generation of keys, let calculate n as,

n = p*q;

phi(n) = (p-1) * (q-1);

d) Then by using password entered during registration, we first convert this password into a value of variable 'e' which can be relatively prime as,

{pwd} -> e ,such that 1<e<phi(n)

e) After evaluating the value of term e we get the Public and Private Key which are used for encryption and decryption respectively.

f) Public Key = PK (n, e) and Private Key = SK (d, n).

g) Public Key (pk) is used for encrypting the information andThen Private Key i.e. Pid is used for decryption of information.

h) This Private Key is Stored in separate Database on Global Server.

3. Due to separate value of term e and random selection of values of p and q it will be hard for attacker to attack on this RSA security and retrieve original data.
4. This single encrypted data using RSA algorithm is converted into double encryption form by applying homomorphic encryption technique.
5. This homomorphic encryption technique creates Secret Key which is used to decrypt the double encryption and original data can be retrieve with this Secret Key.
6. So along with Patients data, Private and Secret Keys which are used for decryption process are also stored in encrypted format on cloud so that if attacker bypass the cloud security firewall he/she will not get actual keys and original data on that third party global server/cloud.

5.2 Encryption Process:

When Patient/Doctor registers himself on application at that time he/she is free to set the password of

his/her choice.

Then, by using this password as 'e' and choosing the value of 'p' and 'q' public key and private key is generated using RSA algorithm.

This public key is used to encrypt the Patient's/Doctor's information and then homomorphism encryption is applied on that already encrypted data so that data should be doubly encrypted and stored on global server.

Example: **E(x1*x2) = ((E(x1)*E(x2))mod N)** which let anyone compute E(x1*x2) from E(x1) and E(x2).

Now on server side Database of Patient and database of doctors will be maintained in encrypted format along with the secret keys are also in encrypted format. So, now server doesn't have any original data but only the encrypted data on it.

5.3 Decryption Process:

In our system, private key which is generated during RSA algorithm is also stored on global server by applying double encryption.

So, the password which used during registration is first encrypted using RSA algorithm and then again this password is doubly encrypted to store on global server.

These singly and doubly encrypted keys are sent to corresponding registered user on his email.

So, when Patient wants to see his treatment information as well as wants to book an appointment then he/she uses his/her singly encrypted key.

When Patient will take an appointment for treatment and meets that Doctor physically at that time Patient uses his doubly encrypted key to decrypt the data which is stored on global server and Doctor can see the previous treatment records of that Patient and update and insert the data according to treatment.

Example: **D(E(x1*x2)) = x1*x2**.

That is when we decrypt double encrypted text we get results as we performed calculation on original data and not on already encrypted data.

6. SYSTEM DESIGN

Use Case Diagram shows Patient and Doctor Interaction with Web Application. It shows how Patient and Doctor first registered themselves on Web Application and then that information is stored on Database1 at Local Server. After registration Patient and Doctor can Login into Application to perform various functions. At Visit Database2 comes into picture from which doubly encrypted information is decrypted into plain text by using Patient's and Doctor's Secret Keys.

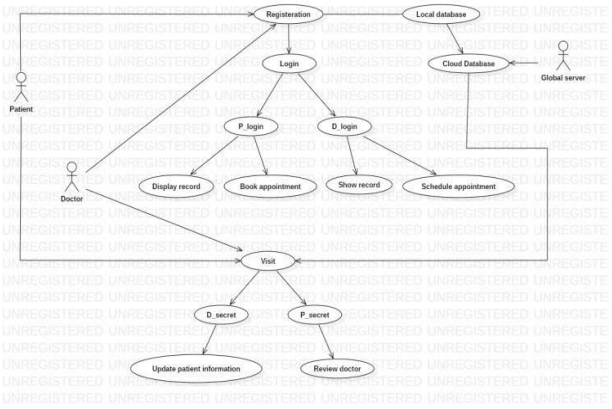
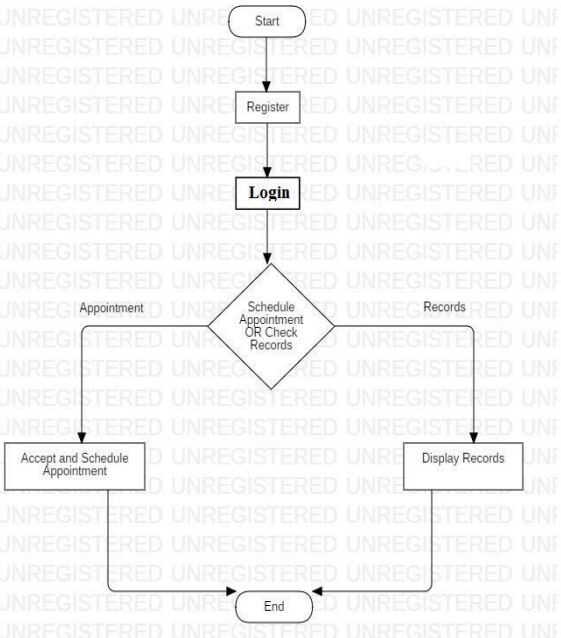


Fig 1. Use Case Diagram



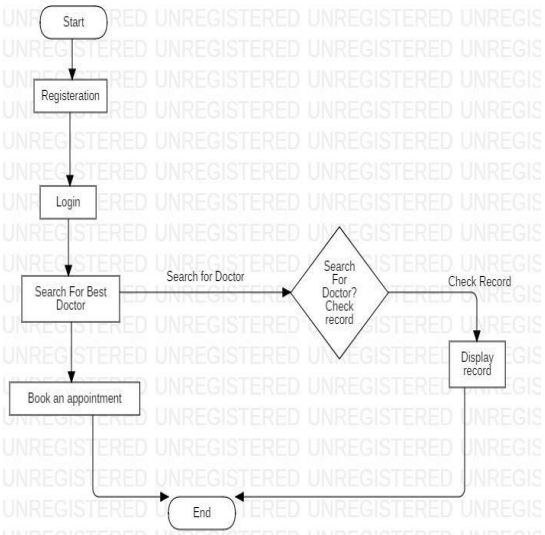
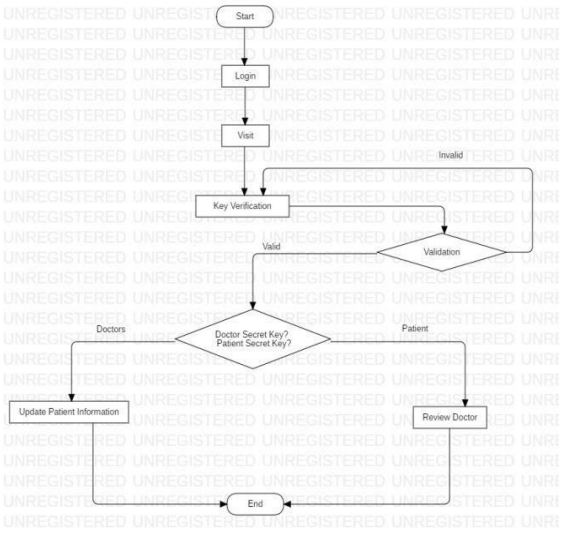


Fig 4. Activity diagram for Patient

Activity diagram show what activities are required to be done by doctor on web application and also show flow of activities from starts to end.

When Patient logged in into the application he/she can search for Doctor based on location and specialization. Also, Patient can check his medical history by using his/her Private Key but he is not authorized to edit/altered his/her medical records on his own. Doctor can check appointment request and send response to Patient with data and time of the appointment.



This activity diagram shows the steps followed by Doctor and Patient during their physical checkup.

Patient provides his Secret Key so that Doctor can check Patients medical records and perform further treatment based on those previous records. Doctor provides his Secret Key so that Patient can give review to that specific Doctor based on his treatment.

7. ADVANTAGES

- Data security is maintained due to use of fully homomorphic encryption.
- Using homomorphic encryption can avoid data breach of cloud data.
- Keys to access data on server are secured as we provide encryption to the keys also.
- Due to review system patient can find best doctor within specific area.
- The authenticity of data is not compromised and it can also be accessed by the authentic user.
- Due to online data storage of medical science field traditional paper base system will get vanished.

8. FUTURE SCOPE

In Fully Homomorphic encryption we can extend the scope of mathematical function so to make it extremely complex for attacker to decipher it and attack on user's data. Fully Homomorphic Encryption is advancement in the field of modern cryptography which overcomes the drawback of traditional cryptographic method and partial homomorphic encryption technique. We extend this concept in the field of medical science to secured Doctor's and Patient's database which will stored on cloud. Due to Fully Homomorphic Encryption, data which will be on cloud will always in as double encrypted format and original data is not present as it is on cloud. This security technique can be used in various different applications related to cloud. So, any type of application which stored their data on cloud can use Fully Homomorphic Encryption technique to secure their data on cloud.

9. CONCLUSION

Some of the encryption systems have multiplicative or additive property and combining both gives fully homomorphic encryption. This allows performing multiplicative or additive operations on cipher text data without having to decrypt it first. The homomorphic encryption is solution to reduce security flaws in the cloud. These techniques have more secured approach of hiding the data from

external attacks. In this article, we show that partial homomorphism is easy and efficient to store and secure data on cloud. But due to new age quantum computers this encryption technique is not much efficient. So we show that fully homomorphism can fill all the security flaws of partial encryption and used to secure data on cloud. We also extend this concept in medical science field to achieve reliable and highly secured communication between doctor and patient.

REFERENCES

[1] EEE paper – Colin Boyd and Christian A. Reuter, "A Guide to Fully Homomorphic Encryption" 2017.

[2] Shraddha Shelar, Deepali Rane, "Reducing Efforts in Healthcare System Using Secure Database".

[3] IEEE paper – Yasmina BENSITEL and Rahal ROMADI," Secure data storage in the cloud with homomorphic encryption" 2016.

[4] THESIS – Zhenfei Zhang, "Revisiting Fully HomomorphicEncryptionSchemesandTheir Cryptographic Primitives" 2014.
WIKIPEDIA Article on "Fully Homomorphism".

[5] SPRINGER article – Diaz Perez, "A Brief Introduction to Modern Cryptography"2007

[6] William P Wardlaw, "The RSA Public key Cryptosystem".