



**SASTRA**  
ENGINEERING · MANAGEMENT · LAW · SCIENCES · HUMANITIES · EDUCATION  
**UNIVERSITY**  
( A UNIVERSITY U/S 3 OF THE UGC ACT, 1956 )

# **Data Preserve Privacy Model for Remote Database System**

Submitted by

**SRI BARANI VASTHAN. V**

**VELMURUGAN.S**

**VISHNUPRIYAN.B**

In partial fulfillment for the award of the degree of

**Bachelor of Technology**

in

**Electronics & Communication Engineering**

**School of Electrical & Electronics Engineering**

**SASTRA University**

**Tirumalaisamudram**

**Thanjavur – 613 401**

**April, 2017**

## **Bonafide Certificate**

Certified that the project work entitled, “**Data Preserve Secured Model for Remote Database System**”, submitted to SASTRA University, Thanjavur by SRI BARANI VASTHAN.V (Reg.No 117004193), VELMURUGAN.S (Reg.No 117004215), VISHNUPRIYAN.B (Reg. No 117004226), in partial fulfillment for the award of the degree of Bachelor of Technology in Electronics & Communication Engineering is the work carried out under my guidance during the period Dec 2016 – April 2017.

**Project Guide**

**[Ms. NITHYA. C]**

**[AP II, ECE, SASTRA University]**

**Submitted for the University Exam held on \_\_\_\_\_**

**External Examiner**

**Internal Examiner**

## DECLARATION

We submit this project work entitled, “**Data Preserve Secured Model for Remote Database System**”, to SASTRA University, Thanjavur in partial fulfillment of the requirements for the award of the degree of “**Bachelor of Technology**” in “**Electronics & Communication Engineering**”. We declare that it was carried out by us under the guidance of Ms. NITHYA. C, AP II, ECE, SASTRA University

Name	Register No.	Signature
SRI BARANI VASTHAN.V	117004193	
VELMURUGAN.S	117004215	
VISHNUPRIYAN.B	117004226	

## ACKNOWLEDGEMENTS

First of all we express our gratitude to **Prof. R. Sethuraman**, Vice Chancellor, SASTRA University who provided all facilities and necessary encouragement during the course of study. We extend our sincere thanks to **Dr. G. Bhalachandran**, Registrar, SASTRA University for providing the opportunity to pursue this project.

We dedicate our whole hearted thanks to **Dr. B. Viswanathan**, Dean, SEEE, SASTRA University for their moral support. We also thank **Dr. K. Thenmozhi**, Associate Dean (ECE) who motivated us during the project work.

We owe a debt of deepest gratitude to our mentor **Ms. C. Nithya**, AP II, ECE, SASTRA University for her continuous support and guidance throughout the process during the pursuit of our project work. Her deep insight in the field and invaluable suggestions helped us in making progress through our project work.

We wish to thank our Project Coordinators, all our teaching and non-teaching staff members of the Department of Electronics and Communication Engineering of SEEE for their support and cooperation. We also extend our gratitude to all teachers who taught us since our childhood days.

We would like to dedicate this work with tremendous love to our Parents for their unlimited, ultra-supportive, encouragement, Sacrifices and unconditional love throughout our entire life. Last but not the least; We would like to mention all our friends who were with us in difficult times. They deserve much love and thanks.

Above all, We thank the Almighty for the Divine Grace we received throughout the research work, without which we could not have completed this work.

# TABLE OF CONTENTS

TITLE	PAGE NO.
<b>CHAPTER – 1 INTRODUCTION</b>	<b>1</b>
1.1 Database and its security	2
1.2 Cryptography	4
1.3 Encryption-the elixir for Security	5
1.4 Why Encryption?	5
1.5 Risk associated with Database Encryption	6
1.6 Encryption and its types	7
1.7 Discussion on various Encryption Standards	
1.7.1 DES	8
1.7.2 Triple DES	8
1.7.3 AES	8
1.7.4 Homomorphic Encryption	9
1.7.5 RSA Encryption	10
1.8 Encryption implemented and its key features	10
<b>CHAPTER – 2 RELATED WORK</b>	<b>11</b>

<b>CHAPTER – 3 PROPOSED METHOD</b>	<b>21</b>
3.1 User Interface Section	23
3.2 Cryptographic Section	23
3.3 Server & Database Section	24
<b>CHAPTER – 4 RESULTS AND CONCLUSION</b>	<b>25</b>
<b>4.1 Results</b>	<b>26</b>
4.2 Conclusion	34
4.3 Future Scope	34
<b>REFERENCES</b>	<b>35</b>

## LIST OF FIGURES

S. No.	No.	Figure Name	Page Number
1	2.1	Symmetric Key Encryption	7
2	2.1	Public Key Encryption	7
3	3.1	Block Diagram	22
4	4.1	Welcome Page	26
5	4.2	Admin login Page	27
6	4.3	Admin Dashboard	28
7	4.4	Admin-Register New Patient page	29
8	4.5	Update Details page	30
9	4.6	User Login	32
10	4.7	View Details-user	33

## LIST OF TABLES

S. No.	No.	Table Name	Page No
1	4.1	Encrypted Data in Database	31

## **ABSTRACT**

Over the years, the need for efficient and secured storage of data has become a top priority due to escalating threats of data manipulation and loss. To counter react such threats, a systematic database needs to be brought into place. Security is the key concern in database system.

The major focus of our proposed project is to develop a secured database model, wherein all data which requires high level of privacy are encrypted. To ensure high level security, public key cryptographic technique is implemented where data imperceptibility is achieved.

In this approach database is resides in Apache Tom cat Server. Server running along with JDK gives the remote access for the database, which permit only authorised user to login and manage data. From the user data set only sensitive data are encrypted and taken to the database. It also provides an option to create an account for the new user as a registration process.

This implementation of secured database is platform independent. Being non specific to any application, it can be used profoundly in the field of telemedicine, e-commerce, government record storage etc.



# **CHAPTER – 1**

## **INTRODUCTION**

# **1. Introduction**

## **1.1 Database and its Security**

A database is a collection of data that is related to a particular topic or purpose. As an example, employee records in a filing cabinet, a collection of sales leads in a notebook, are examples of collections of data or databases. The need for the storing and maintaining the data is much more important, because all the data are very sensitive and essential. So to aid this in a better way, a proper database management system and proper encryption standards has to be followed to ensure security in the database. Coming to the first part, storing data and retrieving it from the database has become much more easier now a days with the enhanced database management system, but when security comes into pictures, various issue has to be taken care and proper authentication, authorization should be handed well. But in general Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment. Apart from various security measures, there is a high probability for intruders to break the security and get into database. So the best way to protect the data from intruders is to follow a well standardized Encryption, so that the data is not directly accessible.

Some of the ways database security is analyzed and implemented include

- Restricting unauthorized access and use by implementing strong and multifactor access and data management controls
- Load/stress testing and capacity testing of a database to ensure it does not crash in a distributed denial of service (DDoS) attack or user overload
- Physical security of the database server and backup equipment from theft and natural disasters
- Reviewing existing system for any known or unknown vulnerabilities and defining and implementing a road map/plan to mitigate them.

The following are some of the key features of the database system

- ✓ Access Control and Authorization Steps
- ✓ Assess Database configuration.
- ✓ Assess platform interaction
- ✓ Secure Communication
- ✓ Patch the database
- ✓ Application specific usage of the database
- ✓ Log and Event review.

In the above mentioned features, Secure communication is the most desired one and the communications to the database should be kept private.

## 1.2 Cryptography

The main purpose of cryptography is to keep the message (or the key, or both) secret from the intruders. The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is a cipher text. The process of turning cipher text back into plaintext is decryption. A Cryptographic algorithm is the mathematical function to perform encryption and decryption. It is also called as Cipher. In general, there will be two related functions one for encryption and the other one is for decryption. Security of a particular algorithm depends on the key which is used to solve the encryption and decryption functions. Cryptanalysis is the art and science of recovering the message without access to the key. An attempted cryptanalysis is called an attack.

Cryptography is widely used in information security for achieving effective communication. There are two types of cryptosystems,

1. Symmetric Key Cryptosystem (SKC) such as Data Encryption Standard (DES), Advanced Encryption Standard (AES). These methods focus on the encryption and decryption of the message using the same key which is commonly termed as Private Key.
2. Public Key Cryptosystem (PKC) such as RSA, Elliptic Curve Cryptosystem (ECC), ElGamal and others, focus on the public exchange of the key. It is also known as Asymmetric Key Cryptosystem, which uses two **keys** -- a **public key** known to everyone and a private or secret **key** known only to the recipient of the message.

### **1.3 Encryption-The elixir for security**

Database are essential for all Governmental records and for the Corporate world since the data to be stored will be sensitive and private which has to be stored in a secured manner .Mostly Encryption is considered as the elixir of security which protects the data in the database from various attacks and intruders.

### **1.4 Why Encryption?**

As far as corporate networks is concerned, it has become more and more open to the outside to accommodate suppliers, customers and partners, network perimeter security is no longer sufficient to protect data. Industry experts have long recommended a “defence in depth” approach by adding layers of security around the data. With the network being regarded as inherently insecure, encrypting the data itself is the best option, often cited as the “last line of defence”.In terms of database security, encryption secures the actual data within the database and protects backups. That means data remains protected even in the event of a data breach. Modern approaches to database encryption, such as the Transparent Data Encryption (TDE) architectures introduced by Oracle and Microsoft, make it easier for organizations to deploy database encryption because TDE does not require any changes to database applications. Various other encryption standards also helps in security such as Advanced Encryption Standard, Data Encryption Standard, Homomorphic Encryption, RSA etc.,

## **1.5 Risks Associated With Database Encryption**

- ✓ Malicious insiders and system administrators could access both encrypted data and encryption keys, giving them access to clear text data, unless keys are deliberately isolated in a dedicated key management system.
- ✓ Applications that have legitimate access rights and yet are infected with malware can still access confidential data.
- ✓ Multiple database instances will typically require access to the same keys, driving up the costs of provisioning and rotating keys in a coordinated fashion.
- ✓ Key loss can render data unavailable, since decryption would be impossible—disrupting business operations.
- ✓ Super-users with broad access rights can subvert and potentially disable encryption controls unless suitable checks and balances are put in place.

It is necessary to take these risk factors into account while designing a secured database and its management. Encryption is always not safe with proper key management system. Good key management avoids disruption and business costs. Conversely, compromising a key can put data at risk and losing a key completely can mean that the information is lost forever.

## 1.6 Encryption and its types

There are two types of encryptions schemes as listed below

- Symmetric Key encryption,
- Public Key encryption.

### Symmetric Key Encryption

**Symmetric key encryption** algorithm uses same cryptographic keys for both encryption and decryption of cipher text.

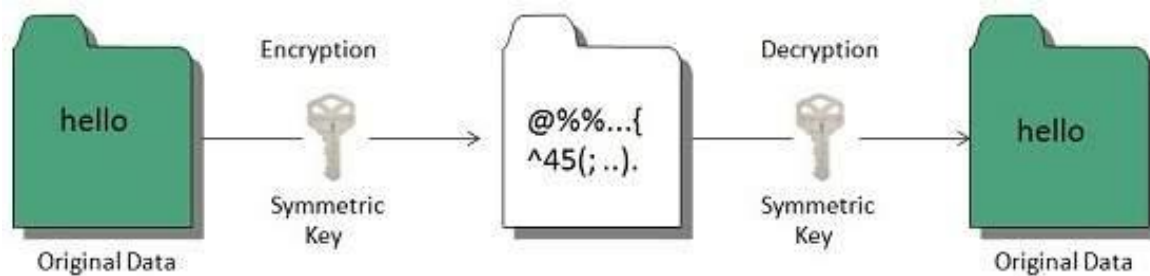


Fig.2.1 Symmetric Key Encryption

### Public Key Encryption

**Public key encryption** algorithm uses pair of keys, one of which is a secret key and one of which is public. These two keys are mathematically linked with each other.

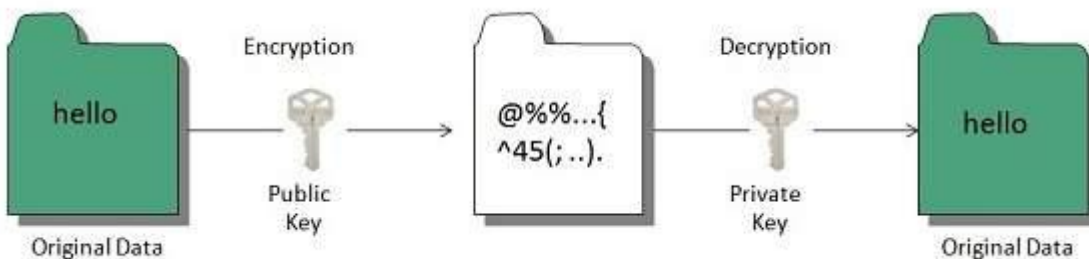


Fig.2.2 Public Key Encryption

## **1.7 Discussions on various Encryption Standards**

### **1.7.1 Data Encryption Standard [DES]**

DES is the original standard that the U.S. government began promoting for both government and business use. Originally thought to be practically unbreakable in the 1970s, the increase in power and decrease in cost of computing has made its 56-bit key functionally obsolete for highly sensitive information. However, it is still used in many commercial products and is considered acceptable for lower security applications. It also is used in products that have slower processors, such as smart cards and appliance devices that can't process a larger key size.

### **1.7.2 Triple DES**

Triple DES, or 3DES as it is sometimes written, is the newer, improved version of DES, and its name implies what it does. It runs DES three times on the data in three phases: encrypt, decrypt, and then encrypt again. It actually doesn't give a threefold increase in the strength of the cipher (because the first encryption key is used twice to encrypt the data and then a second key is used to encrypt the results of that process), but it still gives an effective key length of 168 bits, which is plenty strong for almost all uses.

### **1.7.3 Advanced Encryption Standard**

When the U.S. government realized that DES would eventually reach the end of its useful life, it began a search for a replacement. The National Institute of Standards and Technology (NIST), a government standards body, announced an open competition for a new algorithm that would become the new government standard. There were many competitors including RC6, Blowfish by renowned cryptographer Bruce Schneier, and other worthy algorithms.



They settled on AES, which is based on an algorithm called Rijndael, designed by two Belgian cryptographers. This is significant because they used an open competition to decide on the standard. Also, selecting an algorithm by two non-American developers with no significant commercial interests helped to legitimize this selection worldwide. AES is rapidly becoming the new standard for encryption. It offers up to a 256-bit cipher key, which is more than enough power for the foreseeable future. Typically, AES is implemented in either 128- or 192-bit mode for performance considerations.

#### **1.7.4 Homomorphic Encryption**

Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets. The term is derived from the Greek words for "same structure." Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations -- whether they are performed on encrypted or decrypted data -- will yield equivalent results. Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services.

### **1.7.5 RSA Encryption (Rivest-Shamir-Adleman)**

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm. It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

### **1.8 Encryption implemented and its key features**

To ensure high level security, public key cryptographic technique is implemented where data imperceptibility is achieved. When Public key comes into picture, Homomorphic Encryption and RSA are the two highly secured encryption standards which can be efficiently implemented. But RSA has more advantages comparatively which are listed below,

- Robust to Brute Force attack
- Alphanumeric cipher in RSA
- Mathematical Relation based Key
- Variable key size generation-encryption and decryption.

Even though it has some disadvantages like it need more time for computation, complexity of key generation, Public key leakage, they can be overcome by advanced computational powers and proper authorization for key generation and maintenance.

## **CHAPTER -2**

### **RELATED WORK**

## **2.Related Works**

Encryption algorithms take a plain text stream of data and an encryption key and it generates a cipher text stream of data. They can be broadly classified into two types on the basis whether they use the same key for encryption as well as for decryption. They are

1. Symmetric
2. Asymmetric.

Generally, symmetric encryption algorithms are fast whereas asymmetric algorithms are very slow. This has no effect on the relative security of either types of algorithms. The different performance factors such as key value, computational speed and tunability of as the Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES), 3DES, Digital Signature Algorithm(DSA), RC2 [1]. AES algorithm is better among Symmetric algorithm and RSA algorithm is found as better solution in asymmetric encryption technique. Also, various experimental factors are analyzed. Also, DES algorithm consumes least encryption time and AES algorithm use least memory usage. The encryption time differs in case of AES algorithm and DES algorithm based on the data used for encryption. RSA consume more encryption time and memory usage is also very high. But, output byte is very less in case of RSA algorithm [2].

All the encryption techniques can be used for different real-time encryption. Each technique is unique and has its advantages in its own way. Different encryption techniques can be combined into hybrid form in order to increase the strength of security in applications. However, fast and secure conventional encryption techniques will always work out with high rate of security [3].

Data Encryption Standard is secret key based algorithm suffers from key distribution and key agreement problems. This problem arises since the secret key has to be exchanged. RSA consumes large amount of time to perform encryption and decryption operation. Time consumption of RSA algorithm does not affect its performance in terms of security. The data security provided by the RSA algorithm is always higher and reliable [4].

The key feature of public-key Cryptography is that the encryption and decryption process are accomplished with two different keys - public key and private key. It is also known as asymmetric cryptographic technique, Since the two keys are different. This private key cannot be derived from the public key, that enables the publication of the encryption key without the risk of leaking the secrets.

RSA algorithm is named after its inventors (Ron Rivest, Adi Shamir and Leonard Adleman). RSA has the most significant approach of public key cryptography algorithm and it can resist almost all the known passwords attacks so far. It is the first algorithm that can be used both for data encryption and digital signatures. The security of RSA algorithm depends on the difficulty of decomposition of product of large random prime numbers. In this algorithm, two large prime numbers are used for constructing the public-key and the private-key. The difficulty of decoding the plaintext from signal key and the cipher text equals to that decomposition of the product of two large prime numbers.

RSA algorithm has been used as a possible authentication methods in ISAKMP / Oakley framework. Diffie-Hellman key exchange algorithm is a key component of this framework. In the beginning of a key agreement session, participants communicate by using Diffie-Hellman algorithm and create shared keys which will be used for key agreement protocol of follow-up steps.

The optimal efficiency of an algorithm can be achieved in real time by the combination of symmetric key algorithms and public key cryptography algorithms(i.e.) using a symmetric key cryptography to encrypt the confidential information that needed to be sent, while using the RSA asymmetric key cryptography to send the DES key. This takes advantages of both the two kinds of cryptography, hence combination of high-speed DES and RSA key management mechanism provides high security.

RSA cryptography uses the mode  $n$ , the smallest non-negative complete the remaining lines of operation, where  $n$  is the product of two different primes  $p$  and  $q$  [5].

RSA algorithm is described as following.

First, the generation procedure of keys is as follows,

Randomly generates two primes  $P$  and  $Q$  of length  $K/2$  bit;

Calculate the public key  $publicKey = P * Q$ ; (public Key's length is  $k$ -bit)

Generate a random encryption key  $keyE$ ,  $2 \leq keyE \leq (n)-1$ ,

where  $GCD(keyE, \Phi(n)) = 1$ ;

This is the necessary and sufficient conditions for solvability of the decryption key

$\text{keyE} * \text{keyD} \bmod \Phi(n) = 1$ ,  $\Phi(n)$  is known as the Euler function of  $n$ , the value is

$$\Phi(n) = (P-1) * (Q-1)$$

Calculate the decryption key,  $\text{keyD} = \text{keyE}^{-1} \bmod (n)$ ,  $\text{keyE}^{-1}$  is inverse for the decryption key  $\text{keyD}$ . The formula of the original equation is

$$\text{Key} * \text{keyD} \bmod \Phi(n) = 1$$

Now, the public key, encryption key and decryption key are all created.

Then, the process of encryption of the plaintext and decryption of ciphertext is as follows

Encryption  $C = M^{\text{keyE}} \bmod \text{publicKey}$ ; where  $M$  is plaintext,  $C$  is ciphertext.

Decryption  $M = C^{\text{keyD}} \bmod \text{publicKey}$ ; in which  $M$  plaintext,  $C$  is ciphertext.

It is a complex process to implement RSA cryptography, which involves the generation of prime numbers, large integer modular arithmetic and other mathematical calculations. In RSA cryptography,  $p, q$  are large prime numbers. To achieve this, the most crucial factor is the efficiency in generating large random prime numbers.

Normally, the probabilistic algorithms are adopted in generating large prime numbers. This can be  $p, q$  are two large prime numbers. When seeking primes  $p$  and  $q$  with the method of factorization, then the difficulty is actually the same as to attack to RSA (the decomposition of large composite number. Generally, probabilistic algorithms do not focus on generating prime numbers, but first randomly generate a large odd number, further determine whether this odd integer is a prime number with probabilistic algorithms (this process is commonly referred to as Primality Test).

RSA's security depends on the difficulty of integer factorization. There is no evidence providing that cracking RSA would definitely require making large numbers factorization. Hence, it is not proved that RSA's security is equivalent to integer factorization. If there is an algorithm not rely on large number factorization, it should be able changed into integer factorization algorithm. Currently, a number of variants RSA algorithms have proven to be equivalent to integer factorization algorithm. The decomposition of  $n$  is the most obvious way to attack. Normally, people have been able to decompose more than 140 decimal large prime numbers. Therefore, the module  $n$  must be selected to be large enough depending on the specific usage [6].

RSA be used for authentication as well as for encryption. The generated signature key is safe to a certain level since it is stored only on the user's computer. It is not the same in the case of Hash signature in public key algorithms and hence the security is compromised [7].

Digital signature technology of RSA algorithm is actually achieved by a hash function. Digital signature's feature is that it represents the characteristics of the file. If the file changed, the value of the digital signature will change as well. Different files get different digital signatures. One of the simplest hash functions is an accumulation of a series of binary codes and taking the last few bits as the value. Hash function is open to both sides of data.



While using a network, the main concern is to prevent the data from the security threats. The information and data stored on the portals become higher. Developers and hackers are racing against each other. Developers try to make the web application secure from the threats and the hacker wish to find the loophole, so that it can steal or damage the application or data. Security threats could be with the intent of stealing confidential information, causing deliberate damage, prove capability or simply for the thrill of doing something which most others cannot do. Online Services offers new possibilities to access user data. However, they face the new risks and raise challenges with respect to security and privacy aspects. Ensuring the security and privacy is a major factor in a network environment. A network supported system is designed to improve the standard and effective use and access of user data anytime it is required by owner of the data. This system must ensure the security of user information stored in a network using Encryption techniques such as homomorphic encryption [8].

Organizations have increased their adoption of database systems as the key data management technology for day-to-day operations, the security of data managed by these systems is significant. Damage and misuse of data affect not only a single user, but may have adverse consequences on the entire organization. It is also necessary that data needs to be protected not only from external threats, but also from insider threats. Most security experts believe that insiders are responsible for a vast majority (about eighty percent) of the computer crimes [9].

It is necessary to satisfy the following three requirements

1. Identification and Authentication
2. Access Controls
3. Encryption

Encryption can provide strong security for data at rest, but developing a database encryption solution must take many factors into consideration. Database encryption solutions can be categorized based on their level of trust in the database server, encryption granularity and layer in which encryption takes place.

The level of trust in the database server can range from full-trust, through partial trust to full-mistrust. In the full-trust scenario, the server can perform all operations without any existing threat. In the full-mistrust scenario, since the client does not even entrust the server with clear text queries, the server performs encrypted queries over encrypted data. This scenario corresponds to the database-as-a-service (DAS) model and has significant disadvantages in terms of performance and communication bandwidth. In the partial trust scenario, the database server, together with its memory and the DBMS software is trusted, but the secondary storage that it uses is not.

Most common levels of encryption granularities include *cell*, record, page and table. Finer encryption granularities have some advantages over coarser ones. They are

1. It is possible to encrypt only sensitive data while keeping insensitive data unencrypted.
2. Only relevant data is encrypted/decrypted during a query execution.
3. It is possible to encrypt different parts of the data using different encryption keys.

However, fine encryption granularities are more vulnerable to information leakage and unauthorized modifications than coarse encryption granularities if it is not implemented wisely.

In databases like SQL, one of the most serious and dangerous vulnerabilities in a network system is SQL injection [10]. The aim of SQL injection is to query the database a manner that was not the intent of the application programmer. SQL injection attack is done by inserting a portion of malicious SQL query through a non-validated input from the user into the legitimate query statement. There are several techniques used in SQL injection. Most of them use SQL statement in different SQL injection techniques. Consequently, database system will execute these malicious SQL commands and it leads to SQL injection. A successful SQL injection attack interfere Confidentiality, and availability of information in the database. There is an increased dependence on web applications significantly and it is used in the activities of our daily lives. Hence, database should not be easily destroyed by the intruders [10].

In other familiar databases like Oracle, it has undergone multiple evaluations of its database. In this approach, the users are provided with out-of-the-box security which is the primary requirement. Oracle provides an encrypt/decrypt interface to encrypt especially sensitive data in the database server. Oracle has been enhancing the database encryption, adding in Triple-DES encryption and MD5 cryptographic checksums. Hence, the performance of Oracle is high on par with other database systems.

Apache Tomcat server implements several java EE specifications including Java Servlet, Java Server Pages(JSP), Java JI, and Web socket. It provides a pure Java HTTP web servers environment in which Java code can run. It has several advantages as

1. It is flexible because of ability to pick and choose various modules
2. It has enhanced security

Also, it has a process-based server and it is the one of the main disadvantages, which means each simultaneous connection requires a thread that incurs significant overhead and it is a servlet container (i.e.) it implements only servlets and JSP specifications.

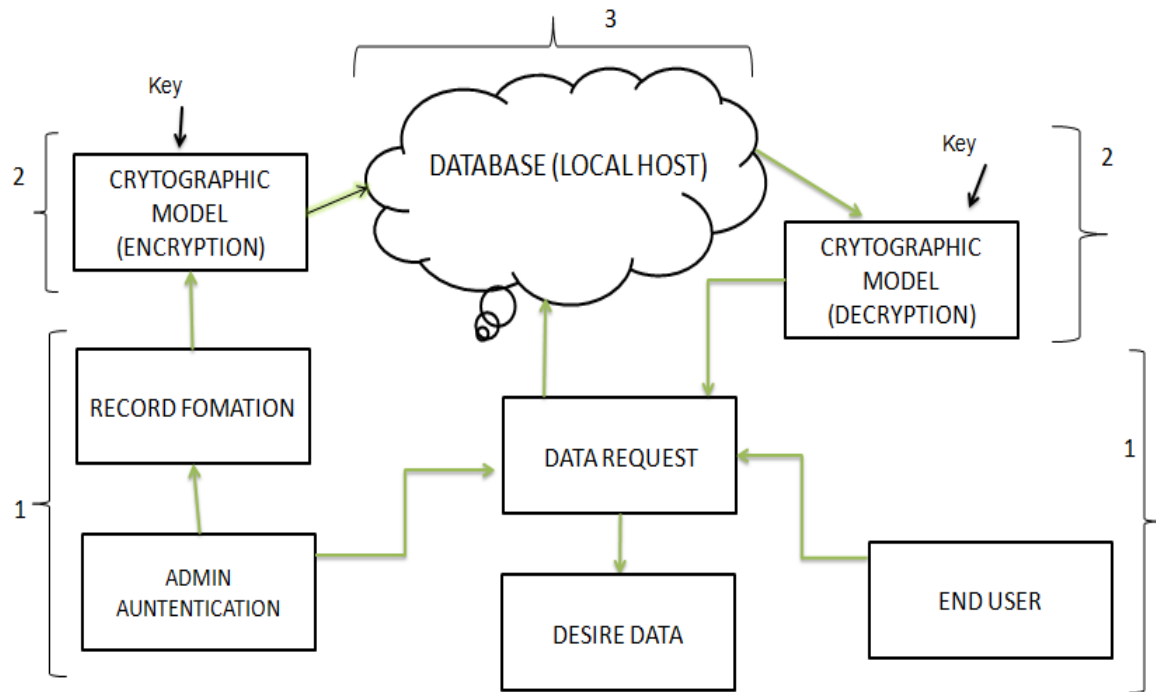
An extra level of security is achieved by running Apache on one physical server, the Tomcat service and the tomcat JSP and servlets on another machine. This should be performed with the Tomcat server behind another firewall only accessible from the Apache server. Stability is one more advantage. Whenever there is failure within Tomcat, the servlets and JSP pages are affected the most, rather making the entire Apache service unusable.

## **CHAPTER – 3**

### **PROPOSED METHOD**

### 3. Proposed Method

#### 3.1 Block diagram of the proposed method



**Fig. 3.1 BLOCK DIAGRAM**

Our secured Database model comprises of three sections which will be described in this chapter. The three sections are

1. User Interface section
2. Cryptographic Section
3. Server & Database section.

### **3.1. User Interface section**

In the User interface section, the new user is provided with an option to create an account as a registration process. This registered user is verified as authorised user by the admin, hence login credentials are provided to this user. Now, this authorised user will get access to the secured database and he will be able to upload his information and manage it. In this process, the sensitive user information that requires high level of privacy are encrypted and the rest of the data are taken to the database.

However, only the authorised user can able to view all the decrypted information from the database. Hence, the registered user has to login again with his credentials and he will be able to view the decrypted information which was related only to him. The secrecy of key has to be maintained very carefully so that security of the database is not affected.

### **3.2.Cryptographic Section**

This Cryptographic Section Comprised of Two distinct models ,one is Encryption and the other one is decryption model. Both the model follows same RSA Encryption Standard algorithm. RSA has many key features when Compared with other public type of encryption. All Public Key Encryption Standard algorithms are implemented by means of Mathematical Relational based key generation, but the main advantage in RSA is its own algorithm complexity for key generation. So breaking its algorithm also requires high computational powers. Also cipher in RSA is Alphanumeric whereas the cipher is Numerical in other encryption standard..

### **3.3. Server & Database Section**

Apache Tom cat Server acts as local web server. This Apache Tom cat Server runs along with java encryption program, and also it provides a remote access for the database to the authorised user to login and manage his information. In order to get remote access to the database, the authorised user should be connected to the same network as the local web server. In this approach database is resides in Apache Tom cat Server. Server running along with JDK gives the remote access for the database, which permit only authorised user to login and manage data. From the user data set ,only sensitive data are encrypted and taken to the database. In this project, the Oracle database is used for the secure storage of the user information. In this database system, the sensitive user information that are entered in the web form are encrypted and stored in the database. This information is decrypted and they are provided to the authorised user who will be able to view and update with a secret key. This secret key efficiently prevents the information on the oracle database from security threats that manipulates and destroys the user information. Well-structured Database queries are management systems are included, so that proper upload and retrieval of data takes place.



## **CHAPTER-4**

### **RESULT AND DISCUSSION**

## 4. Result and Discussion

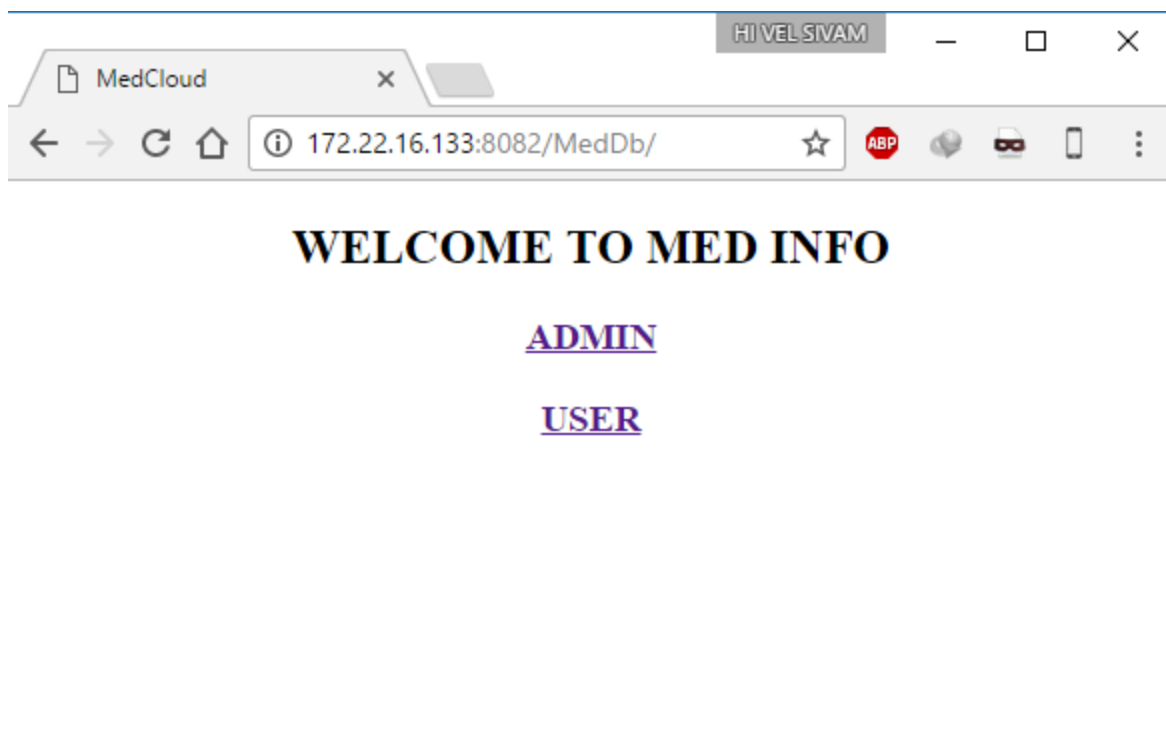
### 4.1 Result

The required results are obtained in the following three models.

1. WEB GUI- Registration & Updating.
2. Database-Encryption Data.
3. WEB GUI -To view Data.(decrypted)

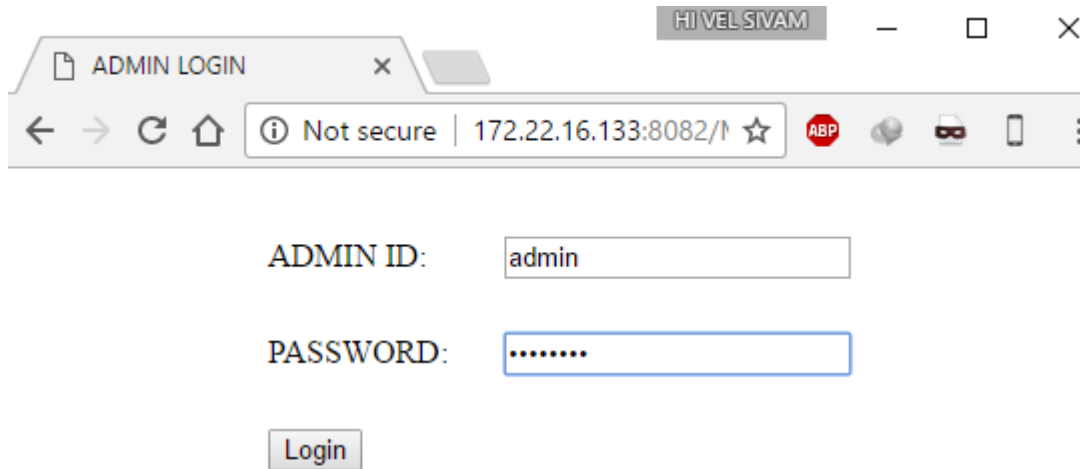
#### 1) WEB GUI- Registration & Updating

- i) It provides two login privileges for Data Administrator and normal user as shown in Fig4.1



**Fig., 4.1 Welcome Page**

## ii) Admin Login Page



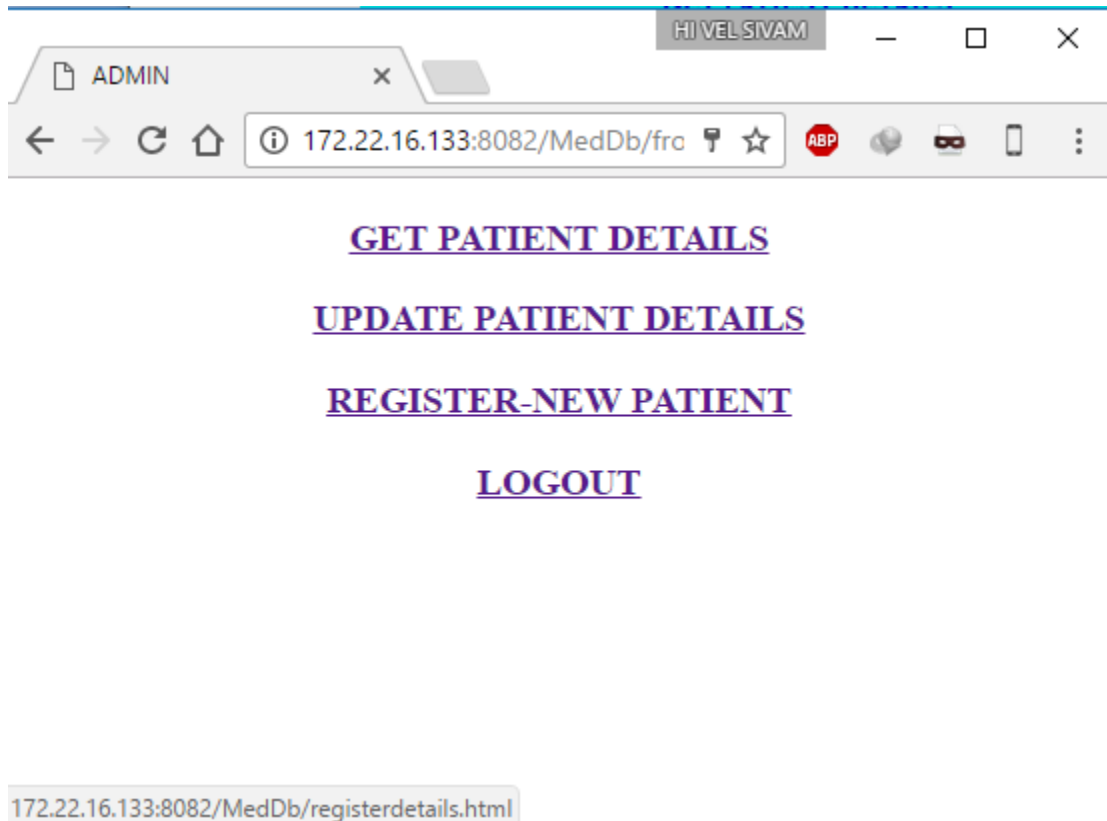
The screenshot shows a web browser window with a single tab titled "ADMIN LOGIN". The address bar displays "Not secure | 172.22.16.133:8082/" with a star icon for bookmarks. The browser's title bar includes the name "HI VEL SIVAM" and standard window controls. The login form consists of two input fields: "ADMIN ID:" with the text "admin" and "PASSWORD:" with masked characters ".....". Below these fields is a "Login" button.

**Fig. 4.2 Admin Login Page**

In this model, as shown in Fig.4.2, the interface is designed in such a way, admin has full authorization to access the entire data in the database, whereas a user can only view his /her own data which was uploaded earlier with the aid of the admin.

### iii) After Successful Login

In this proposed model, secured database is created for Patient Health Record Storage.



**Fig. 4.3 Admin Dashboard**

As shown in Fig.4.3,It has three options,

- Register -new patient
- Update patient details
- Get patient details.

#### iv) Register a New Patient

With the presence of new patient, the admin can only register a new patient with the login password of patient own interest.

The screenshot shows a web browser window with the title 'HI VEL SIVAM'. The browser's address bar shows 'Not secure | 172.22.16.133:8082/'. The page content is titled 'Registration Page'. Below the title is a registration form with the following fields and values:

Field	Value
ID:	117005031
Name:	Bharath
Password:	.....
AGE:	21
GENDER:	<input checked="" type="radio"/> MALE <input type="radio"/> FEMALE
BLOOD GROUP:	B+VE ▼
CITY:	CHIDHAMBARAM ▼

At the bottom left of the form is an 'ADD' button.

**Fig. 4.4 Admin- Register New patient page**

As shown in Fig.4.4, when all the detailed are entered, and on clicking add , all the data are uploaded to the database, in which only sensitive data are encrypted.

#### v) Update Details for an Existing Patient

HI VEL SIVAM

Update

172.22.16.133:8082/MedD

## UPDATE DETAILS

PATIENT ID: 117005031

UNDERGONE OPERATION: ☐ yes ☒ No

SYSTOLE: 120

DIASTOLE: 80

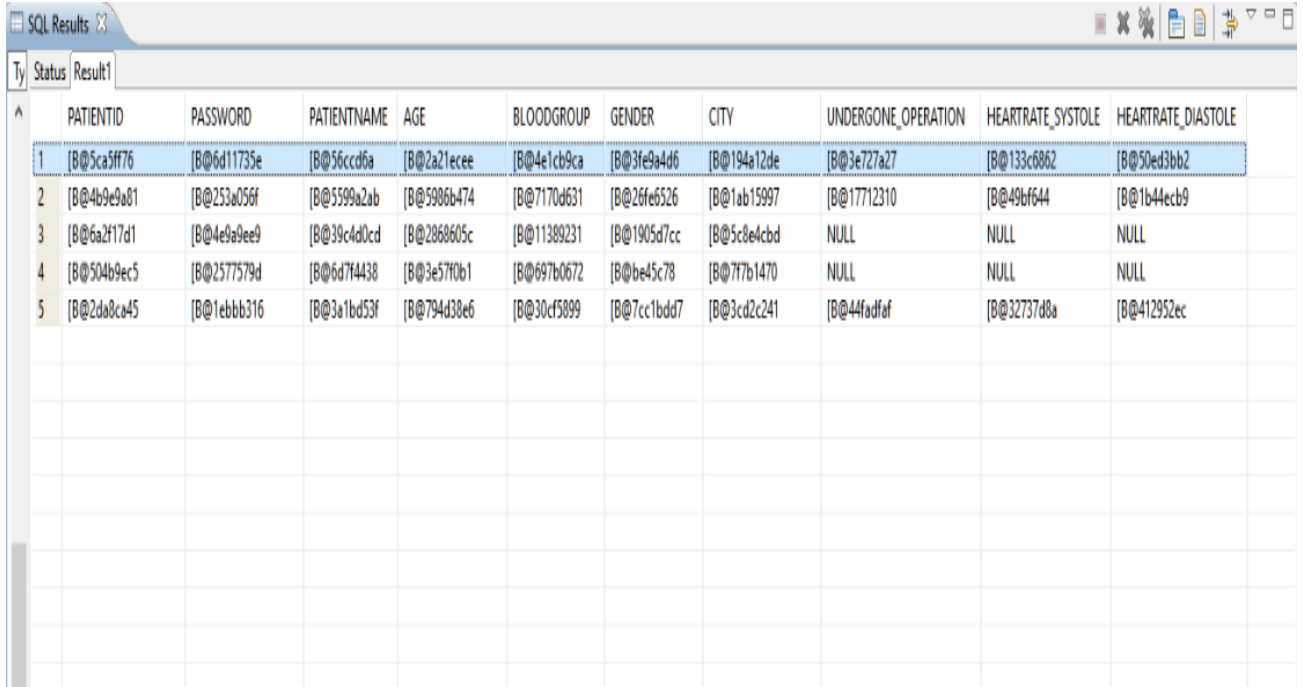
UPDATE

**Fig. 4.5 Update details page**

Here all the data are considered as sensitive data, so all are encrypted and uploaded to the database.

## 2) Database -Encrypted Data

**Table 4.1 Encrypted data in Database**



The screenshot shows an SQL Results window with a table containing 11 columns and 5 rows of data. The columns are: PATIENTID, PASSWORD, PATIENTNAME, AGE, BLOODGROUP, GENDER, CITY, UNDERGONE\_OPERATION, HEARTRATE\_SYSTOLE, and HEARTRATE\_DIASTOLE. The data is encrypted using a hexadecimal-like format, with some NULL values in the UNDERGONE\_OPERATION column.

	PATIENTID	PASSWORD	PATIENTNAME	AGE	BLOODGROUP	GENDER	CITY	UNDERGONE_OPERATION	HEARTRATE_SYSTOLE	HEARTRATE_DIASTOLE
1	[B@5ca5ff76]	[B@6d11735e]	[B@56ccd6a]	[B@2a21ecee]	[B@4e1cb9ca]	[B@3fe9a4d6]	[B@194a12de]	[B@3e727a27]	[B@133c6862]	[B@50ed3bb2]
2	[B@4b9e9a81]	[B@253a056f]	[B@5599a2ab]	[B@5906b474]	[B@7170d631]	[B@26fe6526]	[B@1ab15997]	[B@17712310]	[B@49bf644]	[B@1b44ecb9]
3	[B@6a2f17d1]	[B@4e9a9ee9]	[B@39c4d0cd]	[B@2868605c]	[B@11389231]	[B@1905d7cc]	[B@5c8e4cbd]	NULL	NULL	NULL
4	[B@504b9ec5]	[B@2577579d]	[B@6d74438]	[B@3e57f0b1]	[B@697b0672]	[B@be45c78]	[B@7f7b1470]	NULL	NULL	NULL
5	[B@2da8ca45]	[B@1ebbb316]	[B@3a1bd53f]	[B@794d38e6]	[B@30cf5899]	[B@7cc1bdd7]	[B@3cd2c241]	[B@44fddfef]	[B@32737d8a]	[B@412952ec]

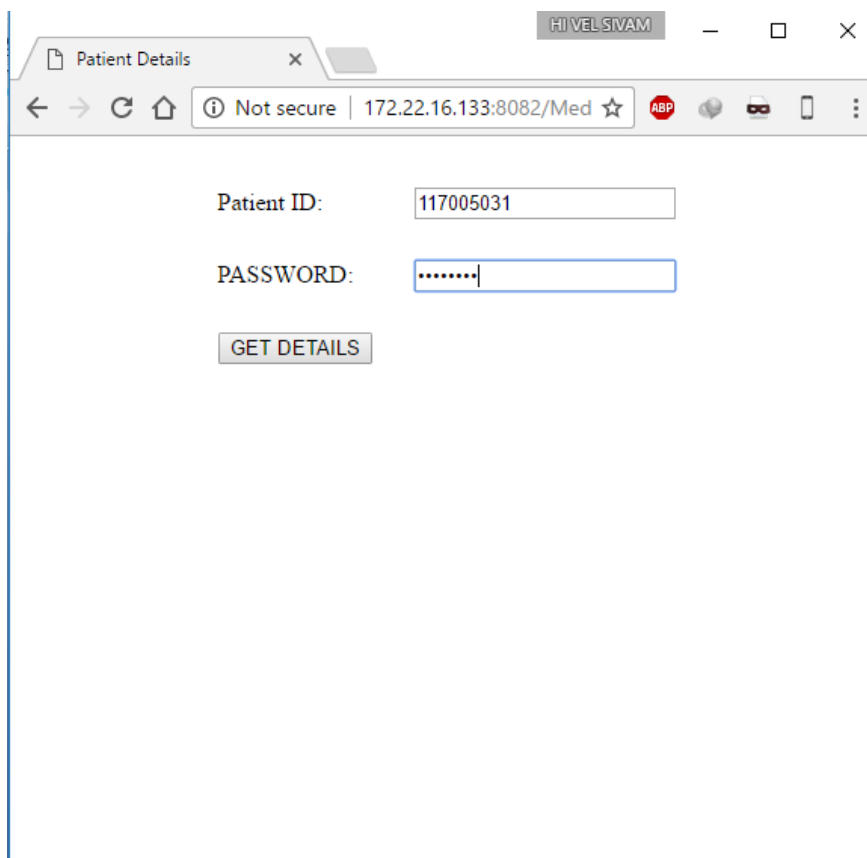
As shown in the above table.4.1,all the sensitive data which are entered in the web GUI are encrypted and uploaded in the database. Whenever a particular information is required (say details of the individual user), only that part of the information is alone decrypted and displayed on the web GUI.

### 3) WEB GUI- To view Data(Decrypted)

Both admin and user can view the decrypted data. But admin can view any individual user's data, whereas user can view only his data.

#### i) User Login page

This also uses JavaScript validation



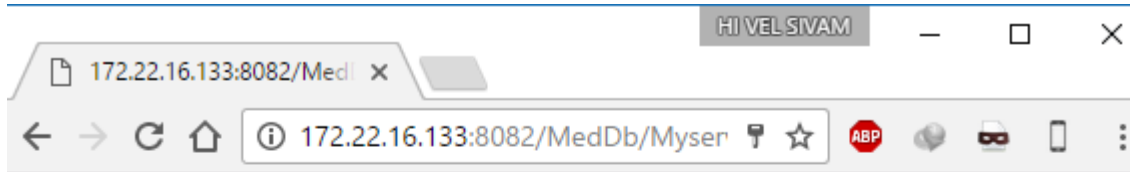
The screenshot shows a web browser window with a single tab titled "Patient Details". The address bar indicates the URL is "172.22.16.133:8082/Med" and the connection is "Not secure". The page content includes a "Patient ID:" label followed by a text input field containing "117005031". Below this is a "PASSWORD:" label followed by a password input field with masked characters ".....". At the bottom of the form is a button labeled "GET DETAILS".

**Fig., 4.6 User Login**

Upon proper login, it will navigate the user directly to view his data.



ii) View data of the user



The screenshot shows a web browser window with the title 'HI VEL SIVAM'. The address bar displays '172.22.16.133:8082/Medl' and the page URL is '172.22.16.133:8082/MedDb/Myser'. The page content is titled 'DETAILS' and displays the following user information:

<b>ID:</b>	<b>117005031</b>
<b>NAME:</b>	<b>Bharath</b>
<b>AGE:</b>	<b>21</b>
<b>GENDER:</b>	<b>MALE</b>
<b>BLOOD GROUP:</b>	<b>B+VE</b>
<b>CITY:</b>	<b>CHIDHAMBARAM</b>
<b>UNDERGONE OPERATION:</b>	<b>No</b>
<b>SYSTOLE:</b>	<b>120</b>
<b>DIASTOLE:</b>	<b>80</b>

[LOGOUT](#)

**Fig. 4.7 View Details-User**

Thus, the encrypted data are decrypted and displayed to WEB GUI for both admin and user as shown in the Fig.4.7.

## **4.2 Conclusion**

Thus our proposed project ensures maximum level of security for the database, with proper authentication procedures, well managed encryption standard, and desired database management system for uploading and retrieval of data. This particular project is more specific for secured database storage for Patient Health Record. Since it has to be available for every individual, Public Key encryption is chosen. In addition to highly secured encryption standard, proper sql queries are chosen in such a way to provide easy management system.

## **4.3 Future Scope**

The implementation of secured database is platform independent and being nonspecific to any application, it can be used profoundly in the field of telemedicine, e-commerce, government record storage etc. It can also be extended as mobile application with simplified connectivity and GUI and easy remote access.

## References

- [1] AL.Jeeva, Dr.V.Palanisamy, K.Kanagaram, "Comparative Analysis Of Performance Efficiency And Security Measures Of Some Encryption Algorithms," *International Journal of Engineering Research and Applications (IJERA)*, ISSN 2248-9622, Vol. 2, Issue 3, pp.3033-3037, 2012
- [2] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication," *IJCST*, Vol. 2, Issue 2, June 2011.
- [3] E.Thamiraja ,G.Ramesh,R.Uma rani "A Survey on Various Most Common Encryption Techniques," *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 7, July 2012.
- [4] Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, "comparative analysis between DES and RSA algorithm", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 7, July 2012.
- [5] J.-H. Hong, "RSA Public Key Crypto-Processor Core Design and Hierarchical System Test," Using IEEE 1149 Family, Ph.D. dissertation, Dept. Elect. Eng., National Tsing Hua Univ., Hsinchu, Taiwan R.O.C., 2000 322-334.
- [6] Steve Burnett and Stephen Paine, "The RSA Security's Official Guide to Cryptography," CA USA Osborne/McGraw-Hill, 2001.
- [7] Dorothy E. Denning, "Digital Signature with RSA and Other Public-Key Cryptosystems," *Communications of the ACM*, 1984.

- [8] Aderonke Justina. Ikuomola and Oluremi O. Arowolo, “Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control,” *International Journal of Computer Networks and Communications Security*, ISSN 2308-9830 .
- [9] P. Boedges. “Air Force mounts offensive against computer crime,” *U.S. Air Force Study quoted in Government Computer News*, 851 ,1988.
- [10] Amirmohammad Sadeghian, Mazdak Zamani , Azizah Abd Manaf . “A Taxonomy of SQL Injection Detection and Prevention Techniques,” Sept. 2013.