Secure Mechanism for Medical Database Using RSA

Pooja[1], Neera Batra[2]

[1]M.Tech., Department of Computer Science & Engineering, MMEC, Mullana, Ambala

[2]Associate Professor, Department of Computer Science & Engineering, MMEC, Mullana, Ambala

ABSTRACT

This paper proposes a concept to implement a real world health database which improves the system for protection of data, restricts the access to data even by the administrator, thus, maintaining the secrecy of individual patient. There is also a need to secure the medical records of the patient. For the data to be transmitted over the network, security is provided by applying encryption on message using concept of RSA. In RSA algorithm, keys are generated online and stored into the database.

Keywords: Encryption, Authentication, SQL, RSA

1. INTRODUCTION

As organizations increase their adoption of database systems as the key data management technology for day-to-day operations and decision making, the security of data managed by these systems becomes crucial. Damage and misuse of data affects not only a single user or application, but may have disastrous consequences on the entire organization. The recent rapid proliferation of Web based applications and information systems have further increased the risk exposure of databases and, thus, data protection is today more crucial than ever. For example, a medical database is a database in which the data about patient is stored. All the details about the patient tests undergoing, prescribed medicines, previous treatment, patient condition and personal information is stored into the database. The user (physician, nurses and administrator) can access the data of their interest and according to the access rights to which they are limited to, access the resources. There are huge numbers of databases that hold confidential information such that people may access those data correlating information from various databases. Access rights for different users must be evaluated and information must be disclosed only to particular extent based on the access rights. Disclosure of confidential information to unauthorized persons may lead to data insecurity leading to dissatisfaction to users.

1.1 Database Security

The most important issues in security are authentication, identification and enforcing appropriate access control. Database system has four main security components: security authentication, authorization, Encryption and multi level access control [4].

Authentication

Usually authentication is realized by password. It is a mechanism that determines whether a user is who he or she claims to be. A user must provide the correct password when establishing a connection to prevent unauthorized use of the database. Passwords are assigned when users are created. A database can store a user’s password in the data dictionary in an encrypted format. Users can change their passwords at any time.

Authorization

Is the process of granting of rights or privileges to the user to have a legitimate access to a system or objects of the system. The purpose of authorization is to supply one secured access point enabling the users to link up to the network once and allow them access to authorized resources.

Encryption

It is the technique of encoding data that only authorized users can understand it. A number of industry standard encryption algorithms are useful for the encryption and decryption of data on the server, some most popular algorithms are RSA, DES and PGP [8].

Access Control

In access control system, users are limited from having complete data access. Policies restricting user access to certain data parts may result from secrecy requirement, or, they may result from loyalty to the principal of least privilege.Medical records are very important information that if sabotage can threat the patient health findings. For example, the intruder or Bad guy have a bad intention to the patient, so one way to execute his plan is to access the medical records of the patient and modify it, replacing the previous or existing findings/records of the patient with the different information that could harm the patient if the physician administers the modified diagnosis. By modifying the records of the patient, the Bad guy can trick the physician by putting different diagnosis. Security threats related to medical databases may affect different areas. Medical databases are extremely important for every organization whether research center, hospitals, colleges, or any other organization. For example, a research center has created a medical database and stored it for future use. In case if any wrong person uses it or hacks it then, it may affect that organization very badly.

2. Related Work

A.A Neto et al. [1] proposed an assessment tool aimed at evaluating the security of DBMS configurations. The proposed tool is simple and effective, and can be used by administrator with very little security knowledge. The evaluation of the tool is done by performing the assessment of four different real database installations based on four well-known and widely used DBMS engines.With the rapid development of Internet, more and more web applications based on database appeared, thus the databases faced different security threats. Because of the SQL attacks, people pay much attention to the security of databases on the internet. Xu Ruzhi et al. [3] proposed a solution by deploying a database security gateway between web server and database server and focused on the research of the attack protection module, including the construction of secure rules library, the process of SQL statements filtering, the improvement and application of Sunday pattern matching algorithm. The database security gateway has been carried out in power industry and has good effect. Leon Pan [4] proposed a method of integrating network security with criterion based access control to handle network security and the fine-grained Web database access control simultaneously. It is important to properly handle network and Web database security issues including authentication, denial of service and fine-grained access control. To improve efficiency, the model adopts two step access control procedure. In the first step, preliminary access control is combined with the firewall function, and in the second step, fine-grained access decisions are determined by the user's digital credentials as well as other factors such as his/her IP address. M. V. Ishwarya et al. [6] implemented the RSA algorithm during data transmission between different communication networks and Internet, which generated the keys by a program prepared in a C # language and then saved these values of the keys in the databases created by SQL Server 2008 R2. A security mechanism on how to secure the retrieving of the data in the database is proposed by Yvette E. Gelogo et al. [7]. Two authentication methods are proposed in this paper, first is the authentication to access the system and second is the authentication to access the data record of the system. On the other hand, an encryption scheme which allows a hierarchical organization of keys to encrypt and decrypt the data stored in the database is proposed by Thomas Hardjono et al. [8]. The scheme uses the same method as the cryptosystem to encrypt and decrypt with additional restriction on the availability of encrypting information to pubic. Its security is based on discrete logarithm algorithm problem NPI. G.Sudha et al. [9] proposed a Pervasive Mobile Healthcare system which focuses on security problems in pervasive computing and provides user the access to multimedia medical record from anywhere and anytime with security being provided by using Elliptical Curve Cryptography(ECC) algorithm. This secured system provides security in delivering the EMR of patients. A Wi-Fi enabled mobile is used to receive or transmit the secured medical data as well as image retrieval. The novelty of the application deals with mobility where the users are able to access the secure information. Weera singhe et al. [10] presented a solution that enables the development of a personal medical record about unconscious patients. The trust delegated medical records are downloaded onto the hand-held mobile devices of the mobile emergency medical personal. The downloaded medical records are used during emergency care and this data should be protected for future software tool that can be used by the emergency medical units in urgent need of sensitive unauthorized distribution of medical data. This paper presents architecture of a mobile security capsule, which enables the trust negotiation to provide a highly secure environment which can be used for the access of highly confidential medical data over the mobile network. S.M.M Rahman et al. [11] proposed three models for secure data exchange in eHealth P2PDBMSs and the corresponding security protocols. The proposed protocol allows the peers to compute their secret session keys dynamically during data exchange based on the policies chosen by them. The proposed protocol is robust against the man-in-the middle attack, the masquerade attack and the replay attack.

3. Proposed Model

The proposed model is an attempt to provide a rich solution to know the details of patient, doctor and receptionist and to hide the confidential data from the outsiders. The main aim of this system is to simplify the procedure while admitting the patient to hospital and to provide a secure and better communication in organization. The security of the database and communication is provided through RSA. In addition to the security through multilevel access rights, encryption of the data is also provided. The proposed scheme uses encryption of data in the database to prevent access by illegal users. Each data element is encrypted and then stored in the database and only the users with the appropriate decryption keys can decrypt any required data. It becomes convenient for the patient’s relatives to know about the details of visiting doctor, treatment details and other details. The implementations of the above modules have evolved user- friendly computerized systems. User is authorized to access the data depending upon permitted user access level. Three levels of users have been proposed depending upon the access permissions given to each user. In the proposed architecture, if a user wants to communicate with other user through internet or by mail, user sends the message in the encrypted (non readable) form using RSA algorithm, and user at the receiving end decrypts the message using a key based on RSA algorithm. The encrypted message, in turn, gets stored into the database. The public and private keys are also stored into the database and retrieved from the database at the time of encryption and decryption from the database.

3.1 System Model

A system model is a conceptual model that describes and represents a system and helps the analyst to understand the functionality of the system. It also shows the interaction between the modules in the system.

3.1.1 Administration Data Flow Diagram

Administration data flow diagram is a graphical representation of the "flow" of data through an administration module. Often they are a preliminary step used to create an overview of the system.

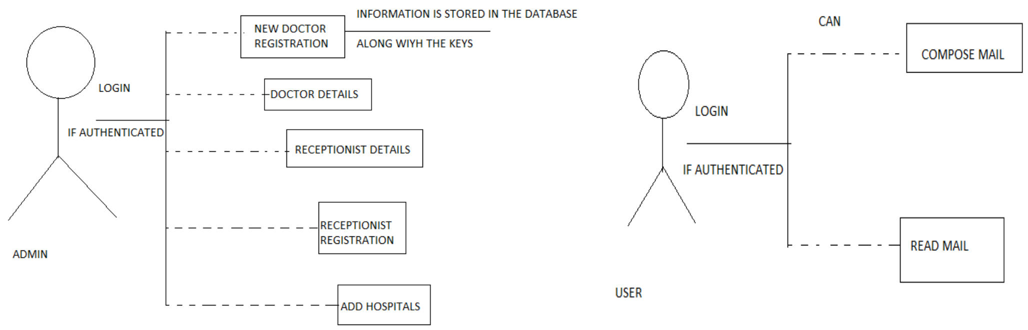


Figure 3.1: Administration Data Flow Diagram

According to this diagram, the user must be authenticated and authorized to the administration. If he is authenticated, then he is provided with the access rights to access the available resources like registration of new doctors, can view doctors details, receptionist details, add hospitals etc. If not, then, access is denied.

3.1.2 Doctor Data Flow Diagram

Doctor data flow diagram is a graphical representation of the "flow" of data through doctor module. Often they are a preliminary step used to create an overview of the system.

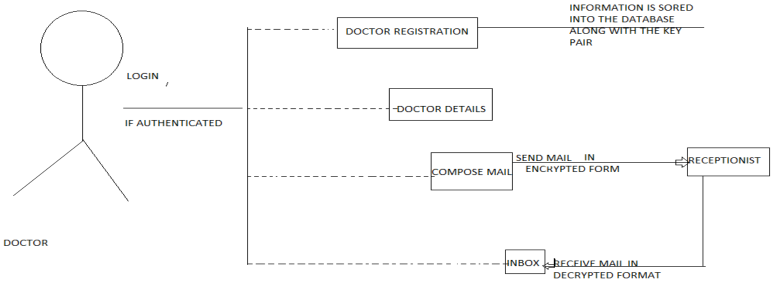

DOCTOR REGISTRATION
INFORMATION IS SORED INTO THE DATABASE ALONG WITH THE KEY PAIR
LOGIN
IF AUTHENTICATED
DOCTOR DETAILS
COMPOSE MAIL
SEND MAIL IN ENCRYPTED FORM
RECEPTIONIST
DOCTOR
INBOX
RECEIVE MAIL IN DECRYPTED FORMAT

Figure 3.2: Doctor Data Flow Diagram

According to this diagram, a doctor can register if he or she is authenticated and authorized to the administration. Then he or she can view the details of the patients and can send and receive the information about his/her patients from the receptionist. The whole communication between the doctor and the receptionist is secured through encryption. The key pair is generated and stored into the tables. These keys are retrieved from the table at the time of encryption and decryption. Encryption is performed with the help of public key of the receiver and decryption is done with private key of the receiver. Database is also kept secured by encrypting the confidential information.

3.1.3 Receptionist Data Flow Diagram

Receptionist data flow diagram is a graphical representation of the "flow" of data through receptionist module as shown in figure 3.3.

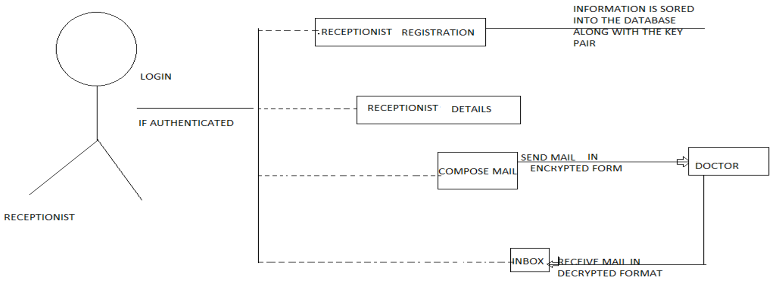

RECEPTIONIST REGISTRATION
INFORMATION IS SORED INTO THE DATABASE ALONG WITH THE KEY PAIR
LOGIN
IF AUTHENTICATED
RECEPTIONIST DETAILS
COMPOSE MAIL
SEND MAIL IN ENCRYPTED FORM
DOCTOR
RECEPTIONIST
INBOX
RECEIVE MAIL IN DECRYPTED FORMAT

Figure 3.3: Receptionist Data Flow Diagram

Figure 3.4 illustrates the flow of how the User (physicians, nurses, database administrator) accesses the medical records of the patient. At start, the user accesses the system by logging in with the username and password. This means that before the User can log-in in the system, he/she must register first in the system. In the registration process, this is the time where all the information about the user is being stored in the system. The user information is stored in a different table separate from the patient's information. This means that during the registration process, the restriction and the access rights on the user are already set. So every time they access the system, the database automatically returns the only possible data that they can access.

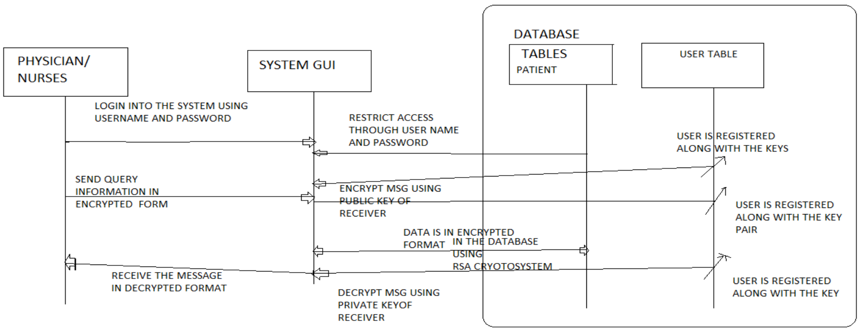

PHYSICIAN/ NURSES
SYSTEM GUI
DATABASE
TABLES
PATIENT
USER TABLE
LOGIN INTO THE SYSTEM USING USERNAME AND PASSWORD
RESTRICT ACCESS THROUGH USER NAME AND PASSWORD
USER IS REGISTERED ALONG WITH THE KEYS
SEND QUERY INFORMATION IN ENCRYPTED FORM
ENCRYPT MSG USING PUBLIC KEY OF RECEIVER
USER IS REGISTERED ALONG WITH THE KEY PAIR
DATA IS IN ENCRYPTED FORMAT
IN THE DATABASE USING RSA CRYOTOSYSTEM
RECEIVE THE MESSAGE IN DECRYPTED FORMAT
DECRYPT MSG USING PRIVATE KEYOF RECEIVER
USER IS REGISTERED ALONG WITH THE KEY

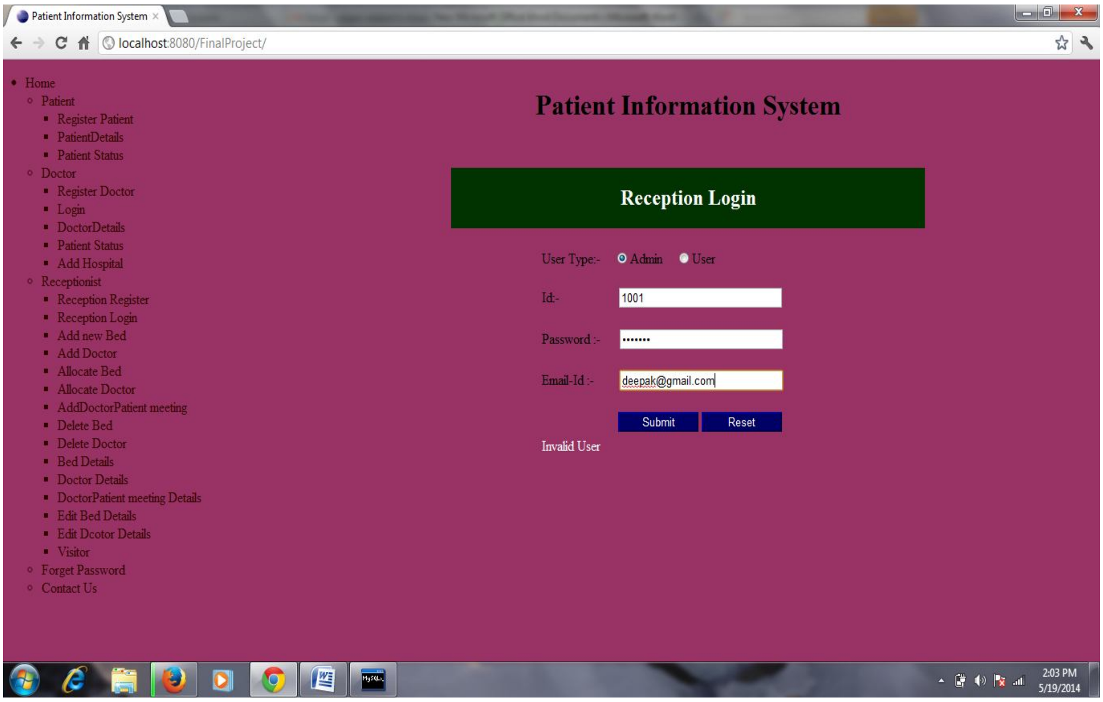
Figure 3.4: Flow of the Proposed Security

4. IMPLEMENTATION

The system model has been implemented using java and database is created and maintained in SQL2005. The benefits of this model over the others are that it is easy to enter the details of the patient and it is easy to retrieve the information of the patient at any time by the doctor and the receptionist even after a number of years. The personal details of the patients are kept hidden from the outsiders with the help of different access rights because everyone is authorized by the administration. This model provides the security at different levels with the help of access rights and provides data integrity, confidentiality, authentication etc. In this model, the information about the patient is encrypted and is kept hidden. Communication is secure because of the information transmitted over the network in a secured way or in an encrypted form.

4.1 Snapshots

Figure 4.1 describes the login page where the receptionist can login himself and use his hospital services.



Patient Information System

Reception Login

User Type:- ● Admin ○ User

Id:- 1001

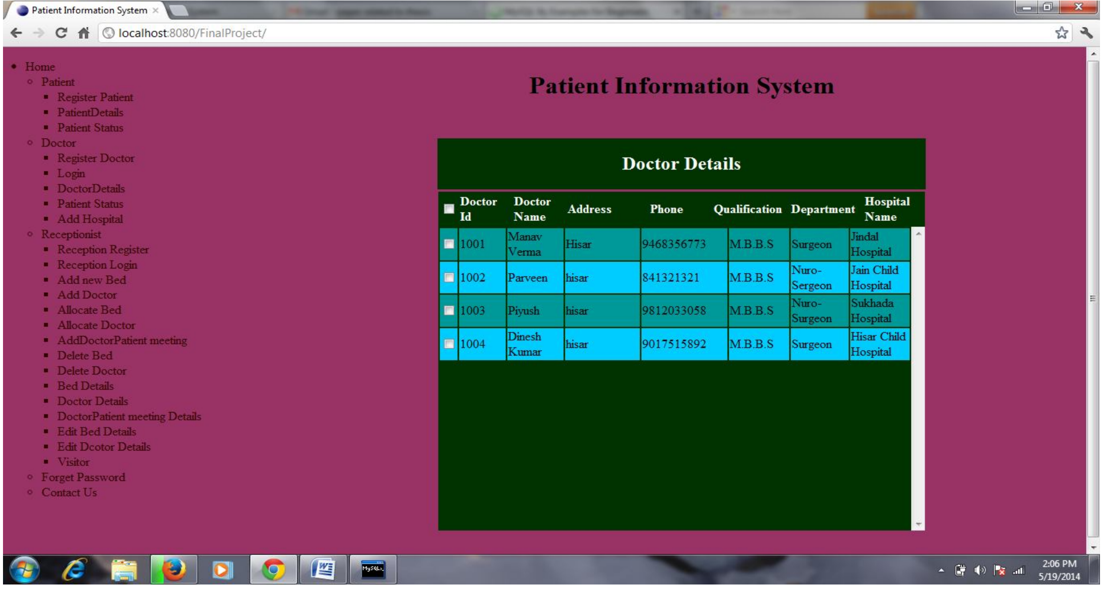
Password :- •••••••

Email-Id :- deepak@gmail.com

Invalid User

Figure 4.1: Reception Login

Figure 4.2 provides the details about the doctors in a particular department to the patients in the respective hospital.



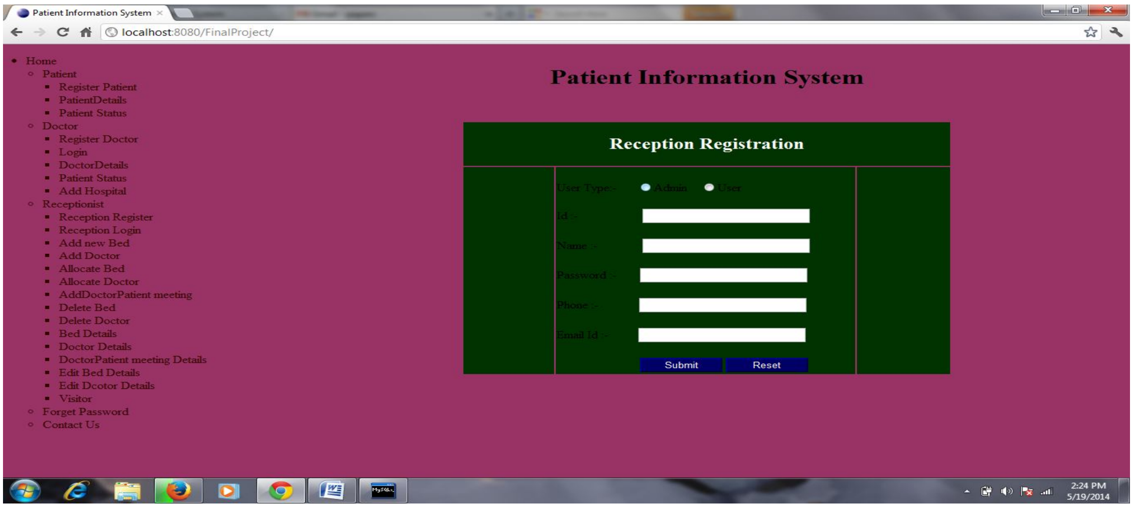
Patient Information System

Doctor Details

□	Doctor Id	Doctor Name	Address	Phone	Qualification	Department	Hospital Name
□	1001	Manav Verma	Hisar	9468356773	M.B.B.S	Surgeon	Jindal Hospital
□	1002	Parveen	hisar	841321321	M.B.B.S	Nuro-Sergeon	Jain Child Hospital
□	1003	Piyush	hisar	9812033058	M.B.B.S	Nuro-Surgeon	Sukhada Hospital
□	1004	Dinesh Kumar	hisar	9017515892	M.B.B.S	Surgeon	Hisar Child Hospital

Figure 4.2: Doctor Details

Figure 4.3 shows the reception registration form. Here, administrator is authorized to register the receptionist details and creates receptionist id and password.



Patient Information System

Reception Registration

User Type:- ○ Admin ○ User

Id :-

Name :-

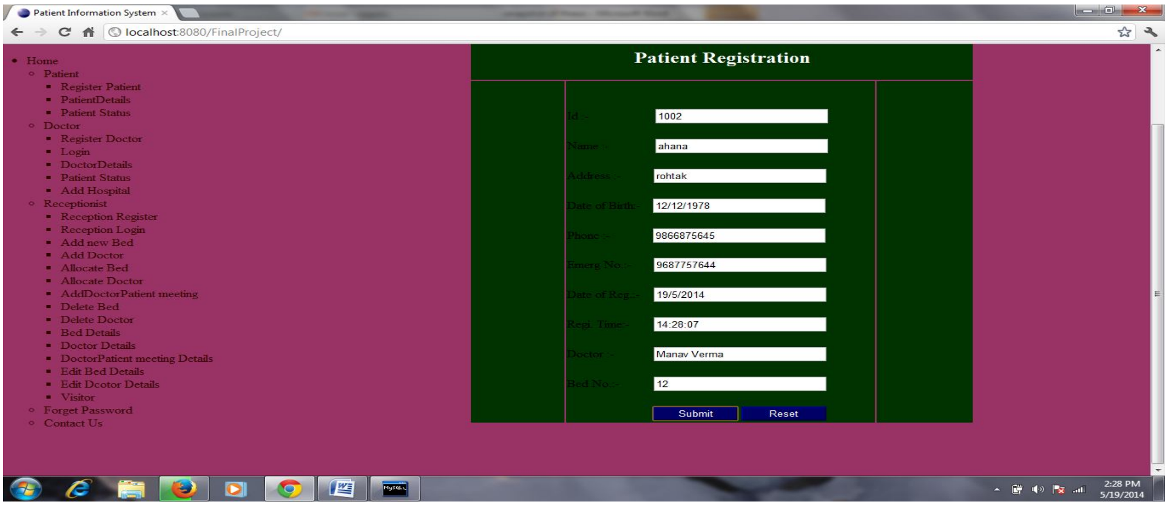
Password :-

Phone :-

Email Id :-

Figure 4.3: Reception Registration

Figure 4.4 shows the patient's registration form. Here, Administrator is authorized to register the patient details.



Patient Registration

Id :- 1002

Name :- ahana

Address :- rohtak

Date of Birth:- 12/12/1978

Phone :- 9866875645

Emerg No.:- 9687757644

Date of Reg.:- 19/5/2014

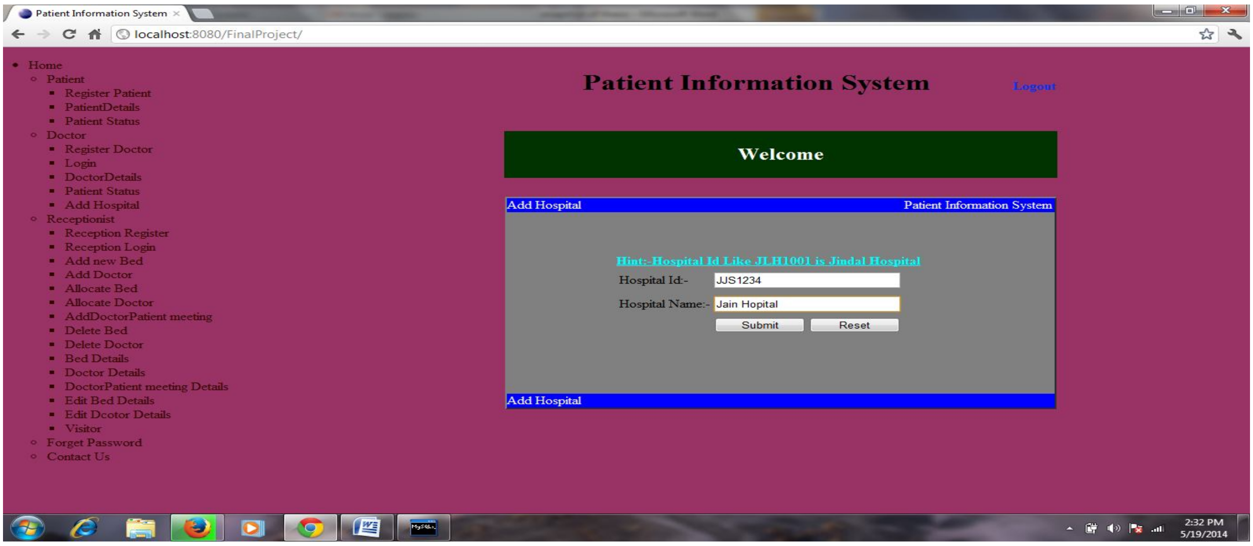
Regi. Time:- 14:28:07

Doctor :- Manav Verma

Bed No.:- 12

Figure 4.4: Patient Registration

Figure 4.5 shows the add hospitals form. Here, Administrator is authorized to add the hospital details and creates hospital id and name.



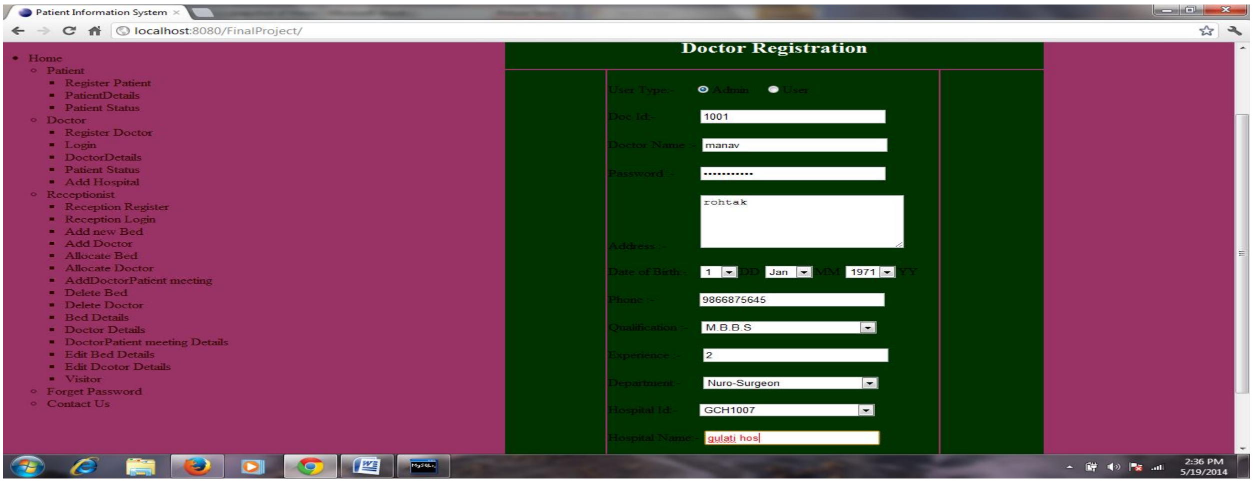
Patient Information System

Hint:-Hospital Id Like JLH1001 is Jindal Hospital

Hospital Id:-	JJS1234
Hospital Name:-	Jain Hopital

Figure 4.5: Add Hospital

Figure 4.6 shows the Doctor's registration form. Here, Administrator is authorized to register the doctor details and creates doctor username and password.

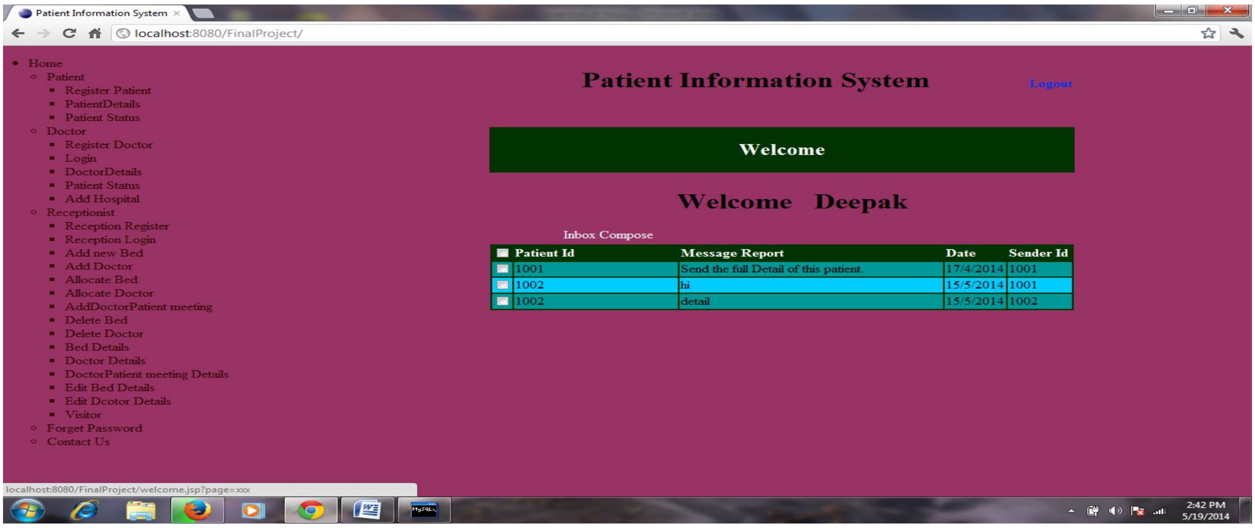


Doctor Registration

User Type:-	● Admin ○ User
Doc Id:-	1001
Doctor Name :-	manav
Password :-	············
Address :-	rohtak
Date of Birth:-	1 DD Jan MM 1971 YY
Phone :-	9866875645
Qualification :-	M.B.B.S
Experience :-	2
Department:-	Nuro-Surgeon
Hospital Id:-	GCH1007
Hospital Name:-	gulati hos

Figure 4.6: Doctor Registration

Figure 4.7 shows the receptionist inbox form. Here, the conversation received from the doctor is stored.



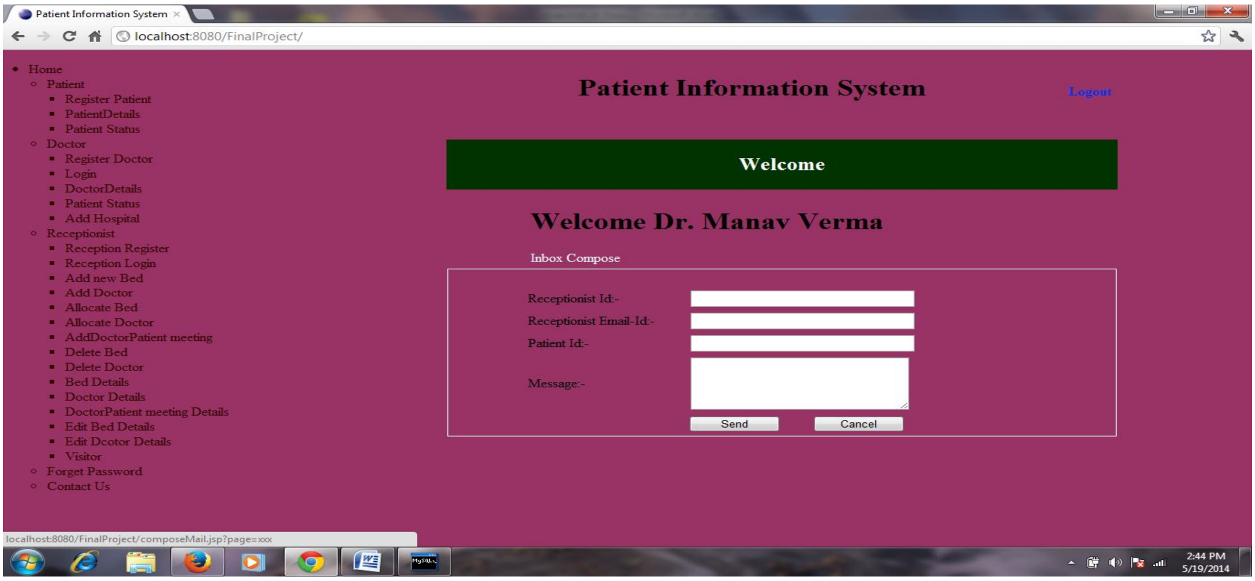
Patient Information System

Welcome Deepak

□	Patient Id	Message Report	Date	Sender Id
□	1001	Send the full Detail of this patient.	17/4/2014	1001
□	1002	hi	15/5/2014	1001
□	1002	detail	15/5/2014	1002

Figure 4.7: Receptionist Inbox

Figure 4.8 shows the compose mail form. Here, doctor sends mail to the receptionist to get the details of patient.



Patient Information System

localhost:8080/FinalProject/

- Home
  - Patient
    - Register Patient
    - PatientDetails
    - Patient Status
  - Doctor
    - Register Doctor
    - Login
    - DoctorDetails
    - Patient Status
    - Add Hospital
  - Receptionist
    - Reception Register
    - Reception Login
    - Add new Bed
    - Add Doctor
    - Allocate Bed
    - Allocate Doctor
    - AddDoctorPatient meeting
    - Delete Bed
    - Delete Doctor
    - Bed Details
    - Doctor Details
    - DoctorPatient meeting Details
    - Edit Bed Details
    - Edit Dcotor Details
    - Visitor
  - Forget Password
  - Contact Us

Patient Information System

Logout

Welcome

Welcome Dr. Manav Verma

Inbox Compose

Receptionist Id:-

Receptionist Email-Id:-

Patient Id:-

Message:-

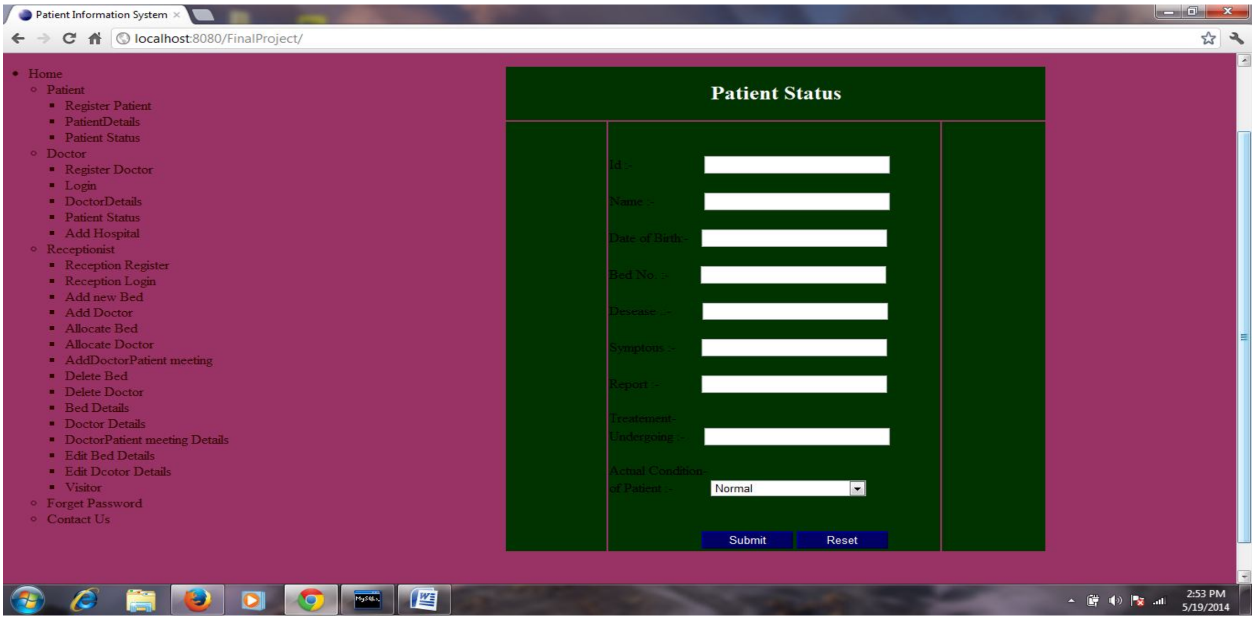
Send Cancel

localhost:8080/FinalProject/composeMail.jsp?page=xxx

2:44 PM
5/19/2014

Figure 4.8: Compose Mail

Figure 4.9 shows the patient status form. Here, patient details and treatment details are updated.



Patient Information System

localhost:8080/FinalProject/

- Home
  - Patient
    - Register Patient
    - PatientDetails
    - Patient Status
  - Doctor
    - Register Doctor
    - Login
    - DoctorDetails
    - Patient Status
    - Add Hospital
  - Receptionist
    - Reception Register
    - Reception Login
    - Add new Bed
    - Add Doctor
    - Allocate Bed
    - Allocate Doctor
    - AddDoctorPatient meeting
    - Delete Bed
    - Delete Doctor
    - Bed Details
    - Doctor Details
    - DoctorPatient meeting Details
    - Edit Bed Details
    - Edit Dcotor Details
    - Visitor
  - Forget Password
  - Contact Us

Patient Status

Id :-

Name :-

Date of Birth:-

Bed No. :-

Desease :-

Symptous :-

Report :-

Treatement-Undergoing :-

Actual Condition-of Patient :- Normal

Submit Reset

2:53 PM
5/19/2014

Figure 4.9: Patient Status

5. Conclusion

After evaluating the performance of access control list and the behavior of the system and users, we can observe that access rights are very important to protect the data from unauthorized access. If there is no security mechanism to protect the data, then user can access the data without permission. Confidential data should be protected from unauthorized access. Security levels protect the data very efficiently from unauthorized access. For the data to be transmitted over the network, security is provided by applying encryption on message using concept of RSA. Security levels also work efficiently in distributed environment. There is a need to secure the medical records of the patient. The use of technologies for remote access to medical records is undoubtedly a convenient way of sharing patient information within and between healthcare facilities. The security measures, in our opinion, are adequate for permitting access only to authorized users without compromising the confidentiality of medical records. In order to have verified the user and give them the right permission to access the records, there are two authentication methods. First is the permission to access the system, then the permission to access the medical records. The restrictions on the access of the medical records are based on the specified rights of the user. For example, physician can access this kind of information and the nurses can only access limited information.

REFERENCES

[1] A.A Neto, M. Vieira, H. Madeira, "An Appraisal to Assess the Security of Database Configurations", IEEE, In the Proceedings of the Conference on Dependability, pp. 73-80, 2009.

[2] Ghassan Gus Jabbour, Daniel A.Menasce, "Policy Based Enforcement of Database Security Configuration Through Autonomic Capabilities", IEEE, In the Proceedings of the Conference on Autonomic and Autonomous Systems, pp. 188-197, 2008.

[3] Xu Ruzhi, GuoJian, DengLiwn, "A Database Security Gateway to the Detection of SQL Attacks", In the Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering, Vol. 3, 2010.

[4] Leon Pan, "A Unified Network Security and Fine-Grained Database Access Control Model", IEEE, In the Proceedings of the Conference on Electronic Commerce and Security, Vol.1, pp. 265- 269, 2009.

[5] Rafae Bhatti, Dengfeng Gao, Wen-Syan Li, "Enabling Policy-Based Access Control in BI Applications", Journal of Data & Knowledge Engineering, Vol. 66, pp. 192-222,2008.

[6] M. V. Ishwarya, Dr. Ramesh Kumar, " Privacy Preserving Updates for Anonymous and Confidential Databases Using RSA Algorithm", International Journal of Modern Engineering Research, Vol.2, pp. 3717-3722, 2012.

[7] Yvette E. Gelogo, Sungwon Park, "A Study on Secure Electronic Medical DB System in Hospital Environment", International Journal of Bio Science and Bio Technology, Vol. 5, 2013.

[8] Thomas Hardjono, Jennifer Seberry, "A Multilevel Encryption Scheme For Database Security", In the Proceedings of ACSC-12, University of Wollongong, pp. 209-218, 1989.

[9] G.Sudha, R. Ganesan, "Secure transmission medical data for pervasive healthcare system using android", IEEE, In the Proceedings of International Conference on Communications and Signal Processing, pp 433-436, 2013.

[10] D. Weerasinghe, R.Muttukrishnan, "Secure Trust Delegation for Sharing Patient Medical Records in a Mobile Environment", IEEE, In the Proceedings of 7th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4, 2011.

[11] S.M.M Rahman, M.M Masud , C. Adams ; K. El-Khatib, H.T Mouftah , E. Okamoto, "Cryptographic security models for eHealth P2P database management systems network", IEEE, In the Proceedings of 9th Annual Conference on Privacy, Security and Trust, pp. 164-173, 2011.

AUTHOR

Pooja did Master of Technology in Computer Science & Engineering from Maharishi Markandeshwar University, Mullana (Ambala) Haryana and Bachelors of Technology in Computer Science Engineering from Panipat Institute of Engineering and Technology (Samalkha) affiliated to Kurukshetra University Haryana. Her research area is Database Security in Healthcare. Her research interests are in access control in distributed database and network security.

Dr. Neera Batra received PhD in Computer Science & Engineering from Maharishi Markandeshwar University, Mullana, Ambala and Master of Technology in Computer Science & Engineering from Kurukshetra University, Kurukshetra. Dr. Neera Batra is in teaching and Research & Development since 2007. She has supervised several M. Tech theses and currently supervising many Ph. d and M. tech theses. She has published more than 15 research papers in International/National journals and refereed international/national conferences. Her research interests are in security, Pervasive Computing, distributed Database