International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Healthcare Management System using Cryptography Encryption (Web Security)

T. Srinivasan[1], Dr. T. Kumanan[2], Ms. Sarika Jain[3], Dr. S. Geetha[4]

[1]M.Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Chennai 600 089, Tamilnadu, India

[4]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

Abstract

In this Covid-19 situation the peoples are very afraid to go to the hospitals in this pandemic situation. So that many of the hospitals the appointment system and the consultant systems are working through in Online websites. Our motive of this project is creating a website to communicate between Doctor and Patient describe about their Issues And add a prescription by the doctor to the appointed patient and main stream of our project is Encrypt the conversation between the doctor and the patient. It will create a trustworthy service to the patient view. Many of the online based hospitality website the customer didn't satisfied about the security of his data. In these days many of the sites have in data leaks through cyberattacks and steal our confidentiality data of the patient so that it leads to the deadliest cause to him. So that we have going to use advance encryption system (AES) method to protect our doctor and patient database. We will give you assurance that our patient details will be secure. So that Patient fill his details and put a lock for his data so that it will be encrypted. In the other scenario the appointed doctor where he will also not be viewing his patient details because it was encrypted one. So, doctor called to the patient and then collect a secret key of his encrypt data so that doctor can decode his patient details and view his information and add a prescription for his patient. So that Hacker cannot be Decrypt the data. And we have another system call option to get online appointment. Our hospitality site will provide a affordable cost for the online Consultant check-up.

1. Introduction

In a modern hospital information system, an online appointment registration system has become a mainstream trend. It brings convenience and reduces waiting time for patients in the hospital. However, it also causes patients' personal privacy disclosure and security vulnerability problems. Effective online medical appointment system (Healthcare Management System) is an online application it allows the patient to book appointments through online registration. A more Convenient Approach Going online is an easy way of life People take resource to online transactions for a safer, convenient and smoother way of life. It is difficult to manage the patients by direct paper appointment. Over the last two decades, the health care has become the most important healthcare service in many developed countries. It is difficult to get appointments by direct contact to the hospital and standing in a queue. the main concept of this project is to get easy appointments through online application which resolves the problem to the patients. With this application the effort to the patients will be reduced which contains the details of the doctor and their available time and the time will be saved for both doctors and patients. the doctor can schedule his own time.

In our project the main speciality is Only the appointed patient Information only doctor can view It and after the process all gets over the particular patient appointment system will be fully erased from the database from his doctor panel only the booking of the appointment but the patient record will be gets stores securely in the database this process will gets routine for the all the doctors list from this website So that Hacker cannot be Decrypt the data. The doctors' profiles are sent to the searcher in the ciphertext. At last, the patient can make an online appointment with the expected doctor. The security analysis demonstrates that the system can achieve data confidentiality and integrity, mutual authentication, secure search, trustworthy, secure his own information.

Index Terms: Online Appointment System (OAS), healthcare, scheduling, web security, cryptographic encryption, privacy.

2. Literature Survey

A. Moffat et.al, This paper presents two different encryption schemes for database. Both schemes use RSA algorithm. The first one is field based encryption system. All fields are accessed by master key of user. Next, represents record-oriented encryption. It uses only one master key. This method applied in subsets and integers group. To provide security to the database is one of the complicated problems. For this, asymmetric crypto system is commonly used. Basically, encryption keys are used to write data in protected fields. Decryption keys are used to read the data. So, it provides the access rights for user. The simple encryption method for database is RSA method. RSA master key pair contains two different keys. Encryption keys are used to represents the right of write operation. The right of read operation is represents by decryption keys. The key pair is maintained by database manager. All rights of fields are combined by RSA master keys. Database manager establishes each field of database in database encryption schemes. Access rights are allocated by using this method. This is used to allocate the access rights depend upon the user requirements. Generally, dynamic data storage is used. Read operation is the most frequent compare to other. Generally, write operations are move to write proxy for approval. The Scheme 2 establishes CRT. This method prevents from the outside attack. It prevents the traffic analysis also. To manage key management problems, both schemes use the RSA master key. Both provides the access rights to user and database security

D. Boneh et.al, major aim of ubiquitous computing is to provide data anywhere, anytime, anyhow only. It is used to enhance the database connections to Internet. And also, it should ensure about the data confidentiality. Day by day, malicious attacks and security threats are increased. So, trusting traditional database security methods is somewhat danger. In this paper, a new method named C-SDA (chip secured data access) is proposed. This control the users' access rights and provides data confidentiality. And also act like a inter mediator between client and encrypted database. This element is embedded in a smartcard. This consists, combined hardware and software. It ensures against attacks. Query evaluation techniques are used mostly

R. Curtmola et.al, day by day, growth of E-business is tremendously increased. So, everybody should be aware about data security and database security. Some RDBMS storage models (such as the N-ary Storage Model) stores records. Offset table is used at the end of the page. It is used to locate the starting point of record. If query is more sensitive, NSM provides tremendous performance. It is used to transfer data to and from secondary storage. This is suitable for online transaction processing. This paper proposes a novel protective model for storage and key

management architecture. It consists of various encryption methods. It ensures high level of database security. In this paper, TPC-H dataset is used with Partition Attribute across (PAX). A page will be divided into mini pages. So, it increases cache performance. A mini-page contains one attribute of record. Depend upon plain and cipher text attributes, the plaintext and cipher text of PAX used to divide the page into two mini pages. So, each record is dividing into two subordinate records. It reduces the cost of encryption as well as storage and computation costs. It takes benefits of NSM. It needs few modifications to page layout.

C. Wang et.al, this paper deals with two major problems. First, security for the encryption. Next, fast performance of query. There are number of methods deals the same. The existing method ensures order preserving encryption techniques are suitable for databases. Compare to other methods this one is very simple and excellent method to build indices. But it creates problems on straightforward attacks. In this paper, a new column-oriented encryption is proposed. It ensures fast indexing operations. Block cipher is applied to encrypt tiny bytes per page. Two cipher texts are compares from the most significant byte. It compares byte by byte. Even though other block ciphers encrypt unit of 8 bytes or more, here it is possible to encrypt byte by byte.

3. Existing System

Online Doctor Appointment system is the system where the users can search the doctors that the needed for and also can take appointment. This system will make easy for the doctors and patients to see their list of doctors and their patients. Find & book appointments with doctors, diagnostic tests, clinics, hospitals.

- Users can even give their feedback to the system administration. Admin can manage doctors, patients. Administration has full authority to add, delete and update doctors and patients. They even add Blood Donor lists and medical doctors.
- The patients can register and search for the doctors basing on the location the list of doctors will be shown and patient can book by selecting the time slots and the admin will confirm the booking so everything is computerized an done very fast which will save time.

Here we can divide this existing system features into 3-types.

- 1.Patient registration system
- 2.Doctor Login panel
- 3.Website Administration

4. Proposing System

In Healthcare management situations we are dealing with the security systems to avoid such kind of data leaks from the Hacker side. So, we have Implement the cryptographic encryption system into the particular pages in such objectives are,

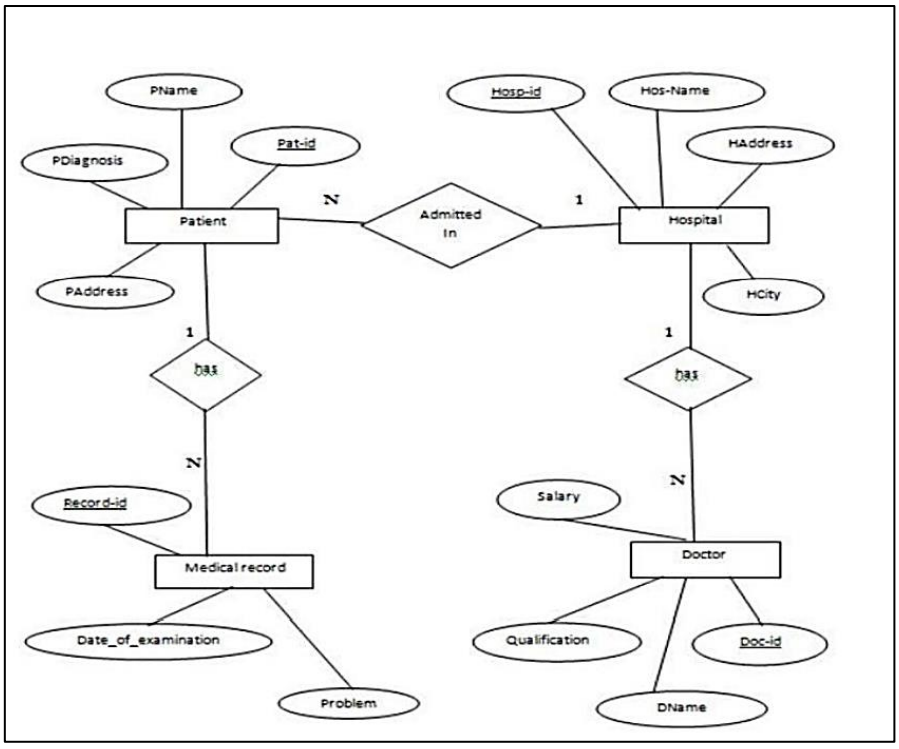
- There is no option to try all the algorithms together in one system.
- There is no privilege for the user to send the encrypted message to other person as a mail.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

- The system will check for any authentication. So that Any user cannot encrypt and decrypt of another data. So that it will only for a Patient and the appointed doctor itself. the third person will see only a encrypt message If he tries a SQL Injection method.
- ENCRYPTION: The user needs to enter a plain text and a key. The plain text will be assigned with a unique id to differentiate each encryption process in the system. A The user can encrypt the plain text using any four of the encryption algorithms.
- DECRYPTION At the receiver side the cipher text has to be converted to the actual plain text. The key will be known to the receiver. It is just the reverse process of encryption.

5. Architecture Diagram

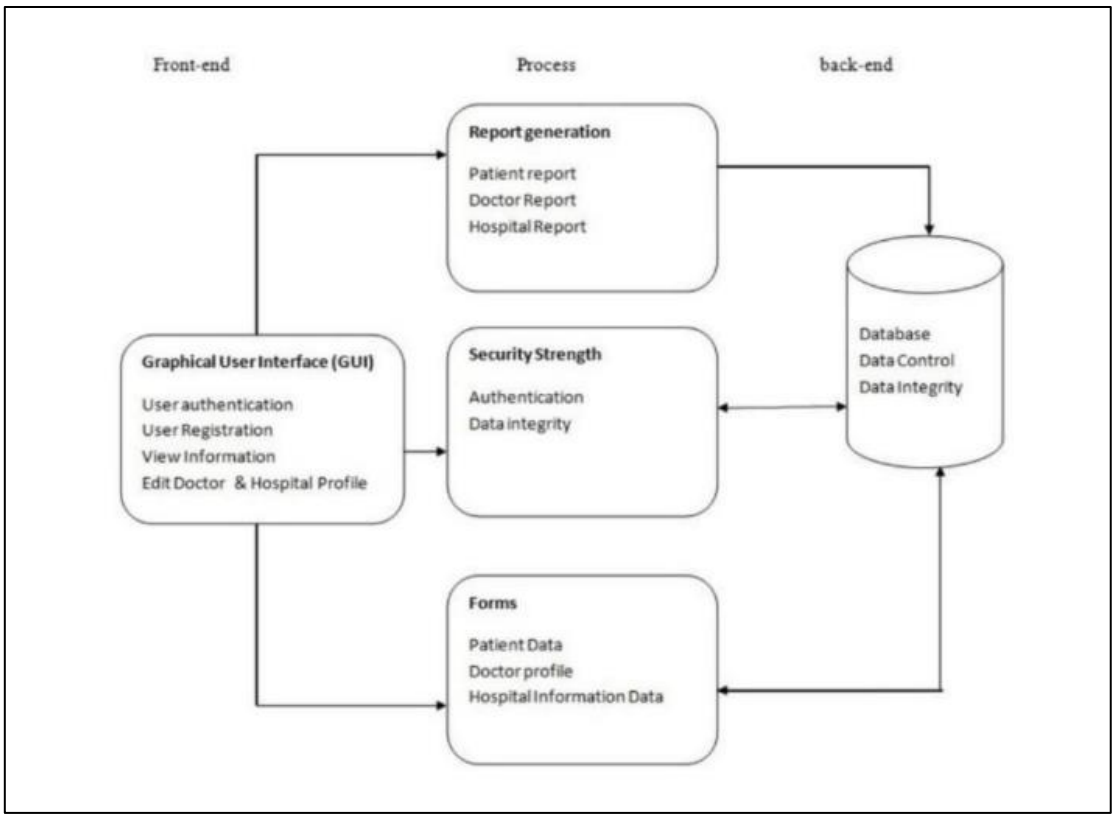
Stored Data of Patient and Doctor on Website



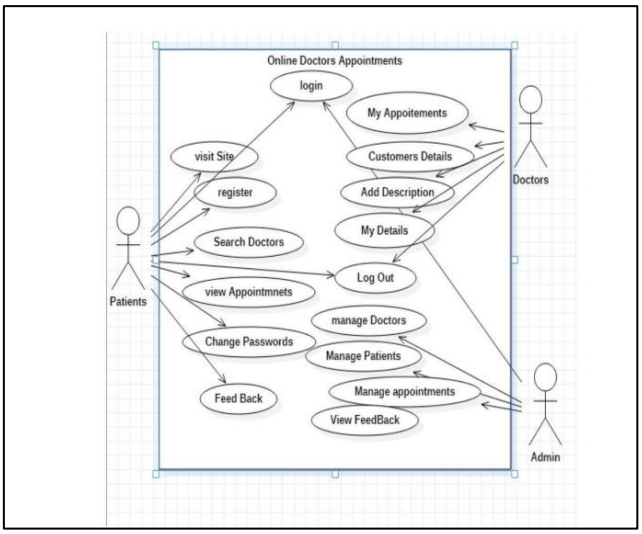
5.1 Architecture Diagram

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Front End and Back-End Process



Online Appointments



6. Modules and their Functionality

6.1 HOME (Portfolio Page)

This page has name of the website and know about such healthcare information in that. And what we done and what we do.

About Us

About us consist of our description of the site and tell us our company story, what we are offering to you.

Medical Doctors List

Lists of the special doctors and what they expertise in that field and shows by the different locations.

Contact Us

Contact us says about the details of our store like (phone no, address, etc.).

User Login

This page shows up-to patient and doctor login credentials field to choose up.

Patient Sign Up

This page ups to new patient to sign up and give his information's such us (name, age, 14 mobile no, address, blood group, email, password)

My Details

This page will show up the patient personal information and also doctors personal information's.

My Appointment

This page for view the appointment system for the patient and doctor view.

Feedback

In this page patient can say up what should be improve and or else give some positive about our website.

Search Doctors

In this page the patient can look up his special and personal doctors nearby his location and book an appointment to it.

My Health

This page shows the field to fill up his disease, disease description, Prescription, and next appointment date **DOCTOR LOGIN**.

This page used to login with doctor details like the credentials will generated by admin and doctor can login using of Doc Id and Password.

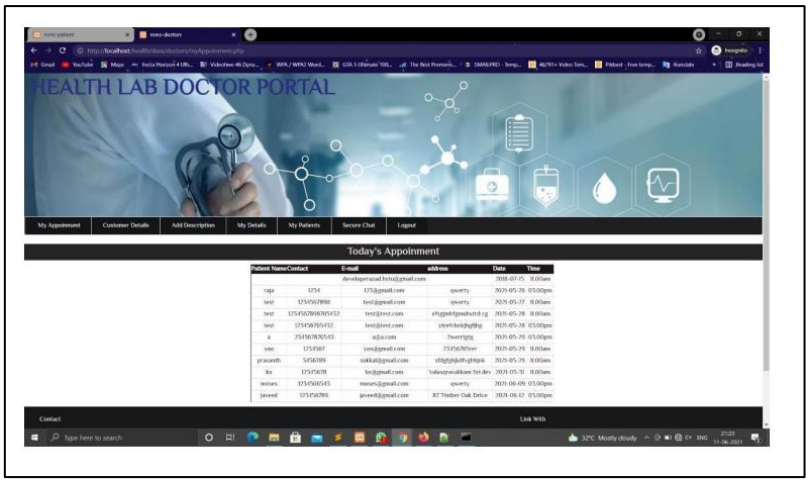
International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Customer Details

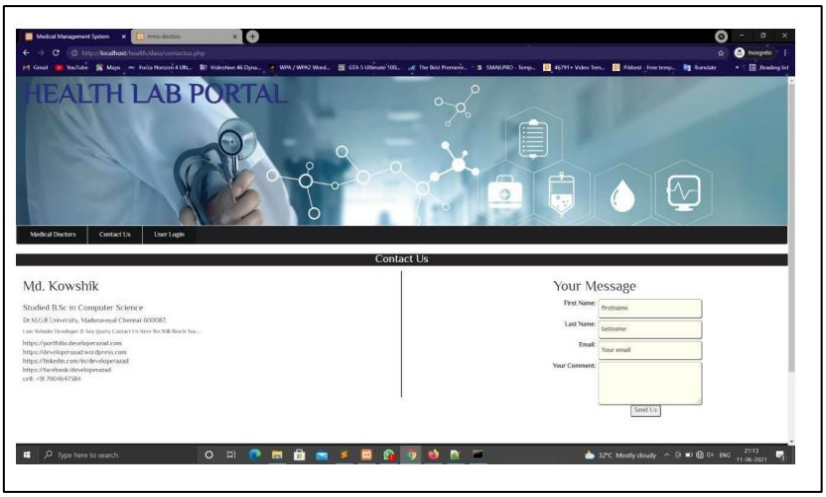
This page will show up in the doctor login page. this page shows patient details of his appointment date time and what kind of disease is it.

MY PATIENTS: This page shows the appointment of the patient details of his disease and disease description it works like consultant support

7. Screen Shots

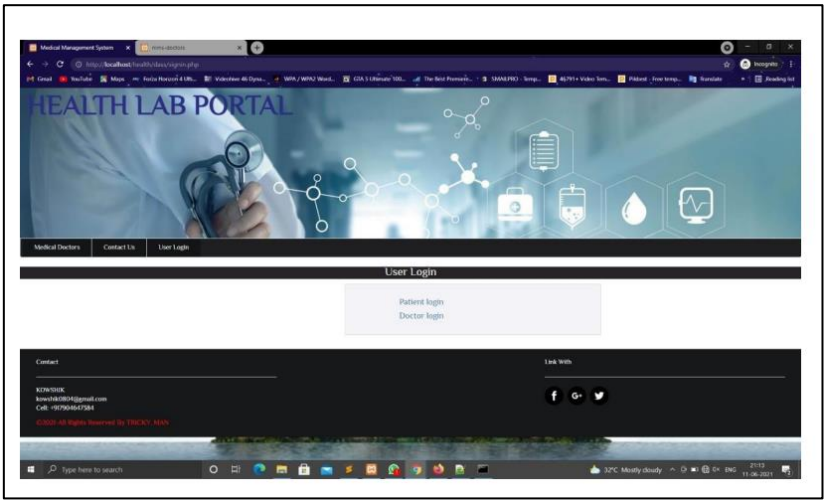


View Appointment Bookings

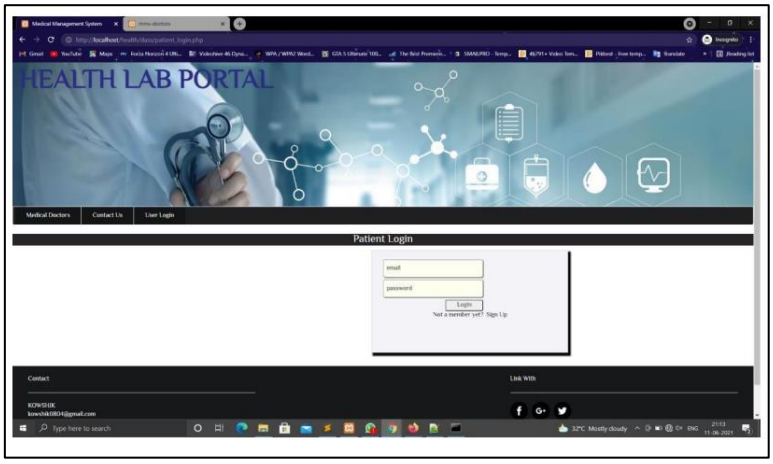


Contact Us

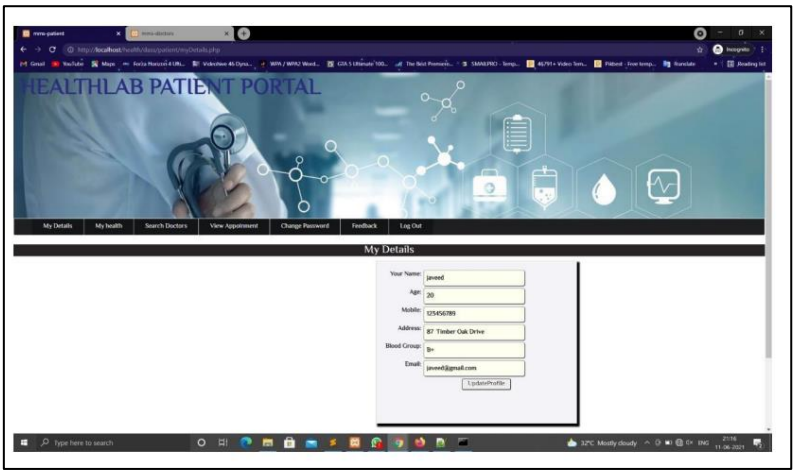
International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



User Login Page

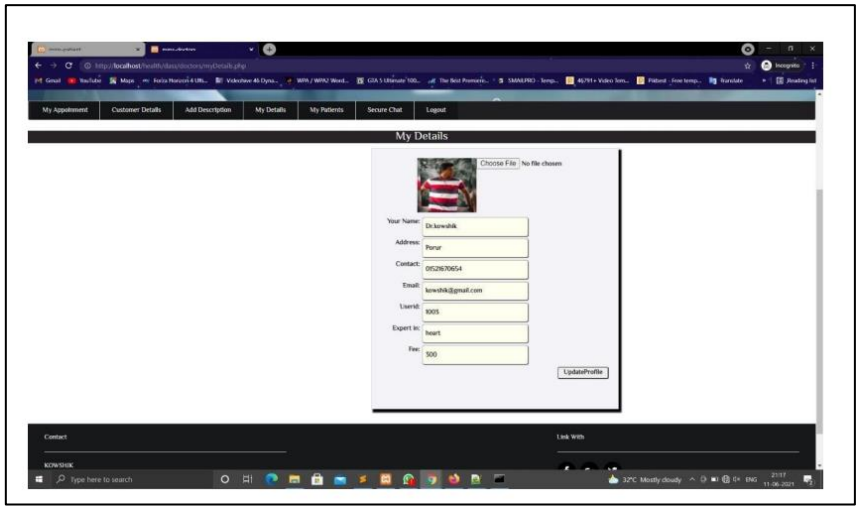


Patient Login

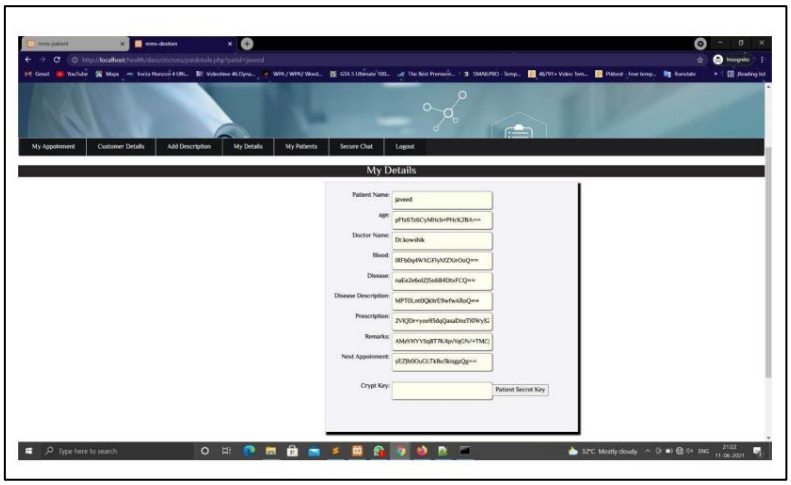


My Details Page

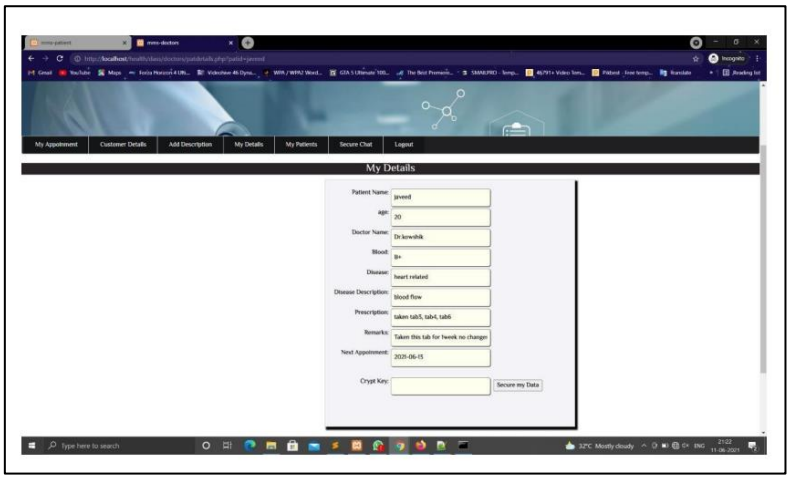
International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



Doctor Info Page

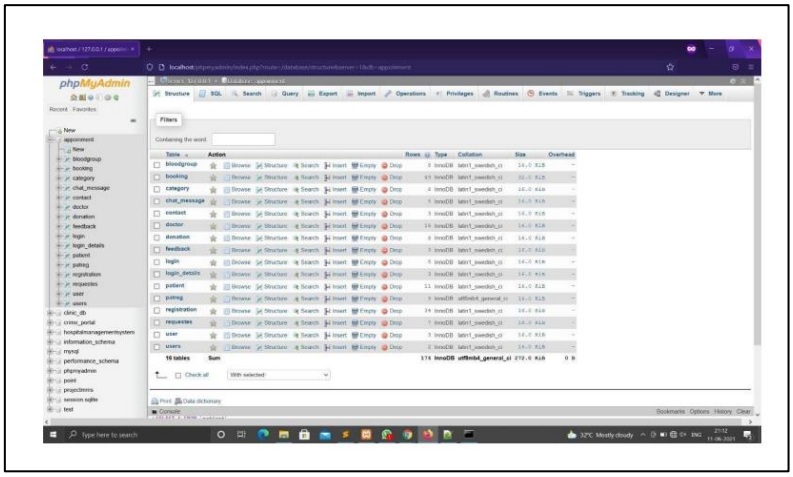


Patient Encrypt his Data using Crypt Key8.



Doctor Decrypt his Data using Patient Crypt Key

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795



Complete Database System

8. Conclusion

The work accomplished during this project can be summarized with the following In this project we have presented a new system for the combination of cryptography implemented in the web based application. we design a secure EHR system to protect patient privacy and enable emergency healthcare. The system is demonstrated to be resilient to various attacks, fulfil the desired functionalities, satisfy the security requirements, and maintain a good balance between security and efficiency. This is a web-based application that overcomes the issue of managing and booking appointments according to user's choice or demands. Here the user can select good doctors by viewing their details and reviews. Hence this project offers an effective solution where users can view various booking slots available and select the preferred date and time. In the appointment system we have secure with the AES algorithm. This system also allows users to cancel their booking anytime. With this application the doctor can alert his own schedule. Hospitals can easily manage their registration and appointment process and monitor the flow of patients to the doctor and with this application the time can be saved to both doctor and patient.

References

1. D. Elizabeth, R. Denning Cryptography and Data Security, Addison-Wesley, City,1982

2. W. Stallings, Cryptography and Network Security, Prentice Hall, 2003

3. Chap2.Block cipher。Chap3.Block cipher modes。Chap9.Public-Key cryptosystems.

4. Digvijay H. Gadhari, Yadnyesh P. Kadam, Prof. Parineeta Suman,"Hospital Management System", IJREAM, Vol-01, Issue 11, FEB 2016

5. Website Reference temp https://code-projects.org/doctor-appointment-systemin-php-with-source-code/ 6. Reference taken for error solving https://stackoverflow.com/questions/52200970/php- aes-128-bit-encryptiondecryption

6. Basic of encryption cipher text https://wiki.openssl.org/index.php/Enc

7. Encrypt code taken as Reference https://gist.github.com/lucymtc/54835badb5f1ac70e3e5f3d3d8fa9cf5 .

8. Frederic P. Miller, Agnes F. Vandome, John McBrewster (December 2009) Advanced Encryption Standard. Publisher: Alpha Press