

Peer Reviewed Journal ISSN 2581-7795

## Healthcare Management System using Cryptography Encryption (Web Security)

T. Srinivasan<sup>1</sup>, Dr. T. Kumanan<sup>2</sup>, Ms. Sarika Jain<sup>3</sup>, Dr. S. Geetha<sup>4</sup>

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

<sup>2,3</sup>Center of Excellence in Digital Forensics, Chennai 600 089, Tamilnadu, India

<sup>4</sup>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.



Peer Reviewed Journal ISSN 2581-7795

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



Peer Reviewed Journal ISSN 2581-7795

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.

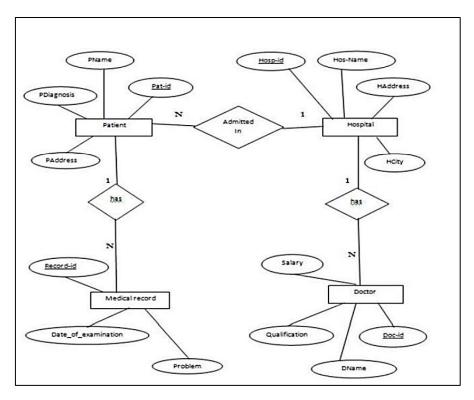


Peer Reviewed Journal ISSN 2581-7795

- 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

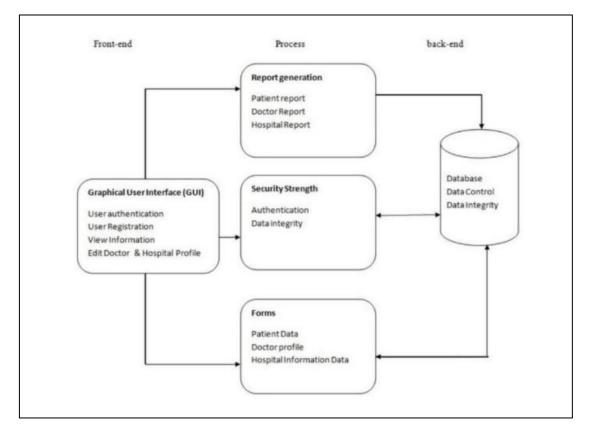
## Stored Data of Patient and Doctor on Website



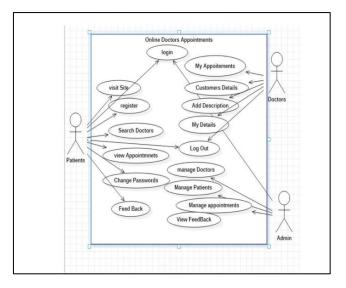
5.1 Architecture Diagram



## Front End and Back-End Process



## **Online Appointments**



## 6. Modules and their Functionality

## 6.1 HOME (Portfolio Page)



## Peer Reviewed Journal ISSN 2581-7795

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.



#### **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

non patient 🛛 🛪 🛄 Anno-ductors 🛛 🛪	× 0					0	
> C . @ Importoathest feedfinities/doctors/myAppoinment.p						÷ (*	Incognito 1
Cenal 🗰 Yochube 🐹 Mage 🛶 Locia Harconi 4 URL. 🖬 Videotwe-	45 Dans	WIR West I Ct	A.S.(Ramate 100. of 114	Reis Provenie - 3 Shirts	1910 - Serge - 40/914	Video Lory. D Pabert - Investoren. In Scanitate .	D Realing for
HEALTH LAB DOCTO	OR POF	RIAL					
		0					
		<b>A</b>					
		2					
		0					
		T		6	3		
		A CONTRACTOR					
	1	b b					
		U		100 100 100	and the second s		
		dy Patients Se	cure Chat Legent				
My Appointment Oustomer Details Add Description	My Details 5						
My Appolement Costoner Details Add Description	My Details						
My Appoinment Contener Details Add Description	My Details		Today's Annoin	ment			_
My Appointment Costoneer Details Add Description			Today's Appoin	1000 C 1000			
My Appointment Constraint Add Description	Patient NameC	ontaxt E-	nd	aldress	Date Time		
My Appointment Costerior Details Add Description	Patient Name O	ordact E4	where and intuigraits	address ors	2018-07-15 If.00am		
Mg Appointment Contenser Datable Add Directiption	Toja	ontoxi E4 de 1254	ndoperated bytuggeoide 1758geoid.com	aldress guetty	2018-07-15 8.00am 2025-05-26 05:00pm		
My Appainment Continuer Datable Add Description	Toja Seul	01/23. E4 de 1254 1254567830	eriger and hotolografic 1758gmal.com test@gmal.com	aldress gently gently	2018-07-15 8.00am 2029-05-26 05:00pm 2029-05-27 8.00am		
Mg Appainment Continuer Datable Add Description	Taja Sent Sent	1254 1254 125492545125452	nelogier anal hetrofigmeitz 175 ägneitzen hetrogenationen testigtest.com	eldress en querty guerty eligibiliteschild (g	2018-07-15 10.00am 2028-05-26 05.00pm 2028-05-27 10.00am 2028-05-28 10.00am		
Ny typeninoni Oustone Datala Add Darchfrin	toga Sent Sent Sent Sent	1254 1254 1254 125450/1990 125450/1990 125450/1990 125450/1991 125450/1991	entigen and hytological a U25 Symall conv test Symall conv test Symall conv test Symall conv test Symall conv	eldress gwerzy gwerzy efiggelitgswiteritig ynwiteleligigtig	2018-07-15 K.00am 2028-05-26 05:00pm 2029-05-27 K.00am 2029-05-28 K.00am 2029-05-28 K.00am		
No Appendixed Contexer Datable Add Discription	Taja Seet Seet Seet Seet	1254 1254 125450/2000 25150/2008/05453 125450/2005453 25450/2005453	enlagerarad botuligerakte U75 gynall om test gynall om test gynall om test ginal om test ginal om test ginal om	did tout off querty genety efigielitysebuild of ytechleidigdig Deerugig	2018-07-15 E.00am 2029-05-26 05:00pm 2029-05-27 E.00am 2029-05-28 E.00am 2029-05-28 E.00am 2029-05-28 05:00pm 2029-05-29 05:00pm		
No Appendixent Consistent Datable. Add Disrectifities	raja raja Seat Seat Seat Seat Seat	25/54/0 22 1254 1256/2000 125150/2946/05452 125150/2956/05452 125150/2055/15 1254/36/2542	entingenerated botoukgeneta entingenerated botoukgenet (255kgenetated entility (2000) feetility (2000) feetility (2000) and (2000) genetated genet	officent energy generaty effoguelitysectuated og synerholdingføg Deserrigits 25156/k/seer	2018-07-15 10.00am 2029-05-26 05.00pm 2029-05-27 10.00am 2029-05-28 10.00am 2029-05-28 05.00pm 2029-05-29 05.00pm 2029-05-29 05.00pm		
No Appendixent	raja raja test test test a vico pracasth	2254 2254 225450/2000 255100/2000 255100/2004/22 255100/205422 255100/20542 255100/20542 255100/20542	and provide the second	ethimi m quarty elegadigashahdig yarihioliyafiy Darrigi 2510500re shigiyiyati-giyiya	2018-07-55 8.00am 2029-05-26 05:00pm 2029-05-27 8.00am 2029-05-28 8.00am 2029-05-28 8.00am 2029-05-28 05:00pm 2029-05-28 8.00am 2029-05-28 8.00am		
Ng Agasimoni Costener Datak Add Donrufute	raja raja test t test t test test test test test	1254 e 1254 23.559/2006 25.559/2006 25.559/2006 25.559/2012 25.559/201 25.559/201 25.559/201 25.559/201 25.559/201	end Distance and botud produce Distance and a series best Symoth com best Symoth com a Symoth com was Symoth com was Symoth com best Symoth com	address querty querty eriggalignulumbrid og ysterkiksignging Dentrygg 2516/2010er stiggingingingingingingingingingingingingi	2018-07-5 10.00am 2029-05-20 05.00pm 2029-05-27 10.00am 2029-05-28 10.00am 2029-05-28 05.00pm 2029-05-29 05.00pm 2029-05-29 10.00am 2029-05-29 10.00am		
Ny kyedenini Contexer Dinde Add Denrytrin	roja roja test t test t test test test test test	9464 E 1254 125577888 125577888 1255783985453 1255887 1255887 1255887 1255887 1255887 1255887 1255887 1255887	nad volkger and hotal) geval a 125 genal com testig genal com testig test com a gio com you genal com wat high so to com wat high genal com mouse genal com	address ans quarty exception exception yourk-bookpeting yourk-bookpeting yourk-bookpeting zitigs/gitige stigg/gitiget.gitige Yolesspeekkow Sri des quarty	2018-07-15 8.00km 2029-05-26 05:00pm 2029-05-27 8.00km 2029-05-28 8.00km 2029-05-28 05:00pm 2029-05-28 8.00km 2029-05-28 8.00km 2029-05-28 8.00km 2029-05-28 8.00km 2029-05-28 8.00km		
No Appelation	raja raja test t test t test test test test test	1254 e 1254 23.559/2006 25.559/2006 25.559/2006 25.559/2012 25.559/201 25.559/201 25.559/201 25.559/201 25.559/201	end Distance and botud produce Distance and a series best Symoth com best Symoth com a Symoth com was Symoth com was Symoth com best Symoth com	address ans quarty exception exception yourk-bookpeting yourk-bookpeting yourk-bookpeting zitigs/gitige stigg/gitiget.gitige Yolesspeekkow Sri des quarty	2018-07-5 10.00am 2029-05-20 05.00pm 2029-05-27 10.00am 2029-05-28 10.00am 2029-05-28 05.00pm 2029-05-29 05.00pm 2029-05-29 10.00am 2029-05-29 10.00am		
	roja roja test t test t test test test test test	9464 E 1254 125577888 125577888 1255783985453 1255887 1255887 1255887 1255887 1255887 1255887 1255887 1255887	nad volkger and hotal) geval a 125 genal com testig genal com testig test com a gio com you genal com wat high so to com wat high genal com mouse genal com	address ans quarty exception exception yourk-bookpeting yourk-bookpeting yourk-bookpeting zitigs/gitige stigg/gitiget.gitige Yolesspeekkow Sri des quarty	2016-07-15 0.000es 2029-05-20 0.500pes 2029-05-27 0.000es 2029-05-28 0.000es 2029-05-28 0.000pes 2029-05-29 0.500pes 2029-05-29 0.000es 2029-05-29 0.000es 2029-05-29 0.000es 2029-05-29 0.000es 2029-05-29 0.000pes		
General	roja roja sed sed u sed s s sed s s s s	2516 2516 2516002006 2515002006 251502006 251502005 25150205 25150205 25150205 2515020 2515020 2515020 2515020 2515020	nad volkger and hotal) geval a 125 genal com testig genal com testig test com a gio com you genal com wat high so to com wat high genal com mouse genal com	obless and querty querty etiggalityschenting ynenheidigtigg hierertyga 25500000000 stigggalityschegtigg verty 456000000000000000000000000000000000000	2018-07-15 8.00km 2029-05-26 05:00pm 2029-05-27 8.00km 2029-05-28 8.00km 2029-05-28 05:00pm 2029-05-28 8.00km 2029-05-28 8.00km 2029-05-28 8.00km 2029-05-28 8.00km 2029-05-28 8.00km	▲ 375 Matricedy ~ 2 × 8 (0 to to: )	2703

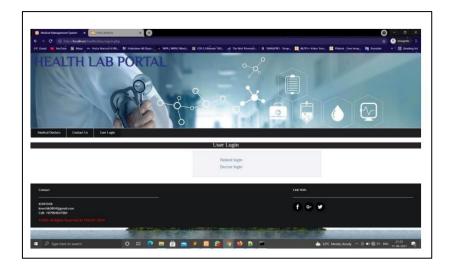
## **View Appointment Bookings**

HEALTH LAB PORTAL	
Ministriker	Contact Us
Ad. Kowshik	Your Message
tudied B.Sc in Computer Science	That Name: forstname
ALCAR University, Maduranoval Cherear-000082. In Motolic Developer II for Query Canter Us Here Ve 900 Block Trac.	Last Name Lastname
n second second per en any specific a second s	Enalt Nor mail
ng-over-engeniaacion graves com typo://incidence.org/developeratal typo://incidence.org/developerates/	Vear Comment
	Send Us

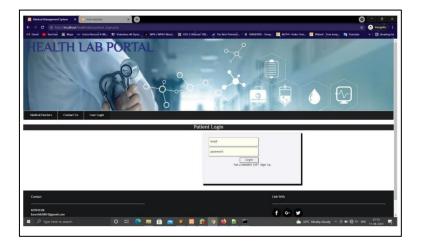
**Contact Us** 



Peer Reviewed Journal ISSN 2581-7795



## **User Login Page**



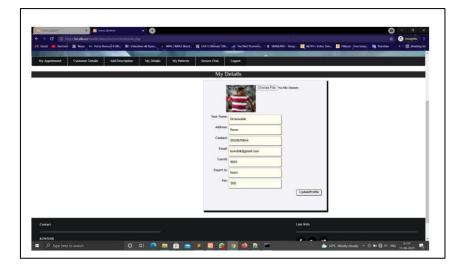
# **Patient Login**



**My Details Page** 



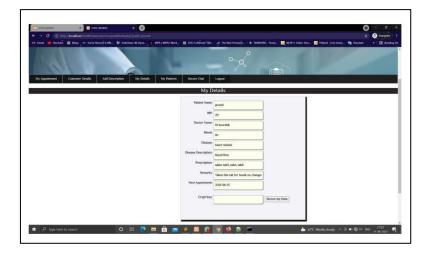
Peer Reviewed Journal ISSN 2581-7795



# **Doctor Info Page**



Patient Encrypt his Data using Crypt Key8.



Doctor Decrypt his Data using Patient Crypt Key



Peer Reviewed Journal ISSN 2581-7795

olahott / 127.00.1 / appoint *														
phpMyAdmin	(M) Serviciare (		Search 🕢 Qu	any iii	Export		P Operat	ions r' P	ristlages 🦪 Routin	. 6 8	rents 🗮 Trigge	cs E Tasking	C Designer 🔻 N	0 X lore
-	Filters													
apportent	Containing the wor	a												
+ > bloodgroup	Table a	Action						en (j) Type	Collation	Size	Overhead			
- e booking	bloodgroup	*	Browne   Structure	R Search	Fi Inaet	豐 E reply	C Drop	t timoDi	a start_swedsh_ci	14,0 818				
+ y category	D booking	*	Theorem 24 Structure	in Search	Sel inset	M Freety	Chep .	4.5 III:600	ant, swellsh, ci	12.0 812				
end_message	Category		Dowse 🖗 Structure	ing Search	Fi inset	Empty	Drop	a impDI	atin1_swedish_ci	16.0 His				
doctor	C shat_message	\$2	Dowte je Stucture	it Search	H insert	<b>種 Engly</b>	O Deep	# innoDi	latin1_swedish_ri	36-2 Xit	(			
+ je denation	contact	* 1	Browse [4] Structure	R Sciett	gi traet	Emply	Drop	1 mouDI	allent_seedesh_cc	14.0 818				
- / feedback	dector	*	Bowe Status	# South	Fr Intert	Empla	O Drop	38 imaDi	is_int_section_cr	1610-818	L -			
- je login	denation.	* 1	Drowse je Structure	ing Search	H innert	M Enerty	Crop	# itroff/	is_dabase_finite_fi	34-0.848				
- / login_details	Needback	*	Broate je Structure	# Search	gi smeet	Emply	O Deep	3 innofil	intent exercises of	15,0 811				
	🗆 legin	* 1	Decese 12 Structure	in Seatth	Bi insert	M Cripty	Chicp	8. innaDi	is_hist_seedah_ci	16.0 818				
+ je registration	login_details	*	Bowe & Studies	A Search	Si kroust	#Entry	@ Dep	A involt	indebook_findef F	16.0 15				
- X mquestes	patient	*	Browse 54 Structure	R Search	H boot	Empta	Orep	11 involt	a latent_sweetist_ci	10.0 Rig				
* /r user	D parent	*	Provent 2 Sectors	A Seatth	Fi Iniart	ME Frees	O Deep	Dorni e	in althebt, personal, et	IS IS A DEST				
in- clinic db	registration	*	Browse 34 Structure	in Search	St inset	BE Erepty	C Deep	24 InnioDi	atest_sweeksh_ct	16.0 848				
in g crimi_portal	reguestes	*	Bowse je Souchare	a Search	Hi Insert	WEnter	O Drop	Y impoDi	latin1_swedish_ci	10.0 #15				
hospitalmanagementsystem	U vser	*	Drowse 14 Structure	R Search	H losert	Errory	Drop	3 innoDI	latin1_swedish_ci	10.0 818				
in information_schema	L users	*	Brown > Seatter	- Selach	Finan	1 Emply	O Drop	I impDi	i ideit_seedub_ci	16.0 215				
performance_schema	10 tables	Sum						174 InnoD	B utflmb4_general_ci	272.0 Hid	0.8			
er-a phonyadme er-a poet	1_ [] Check	sl.	With selected											
ill session adde	SPIRE BORN DE	tomary												
in is test	Conside												Bookmarks Options	History Clea

**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-phpwith-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

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

- 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