REPORT

On

**“Hipaa compliant database app (doc-mobile)”**

**Department of Computer Sciences and Information System**

By,

Mayur Sanjay Potdar (50155714)

Jared Dickinson()

CSCI 581

PROJECT REPORT



Guided by,

**Dr. Jinoh Kim, PhD**

Assistant Professor, Computer Science Department

Coordinator, Computer Science Graduate Program

Texas A&M University-Commerce

2600 South Neal St., Commerce, TX 75428-3011

E-mail: Jinoh.Kim@tamuc.edu

Web: http://faculty.tamuc.edu/jkim/

|  |  |
| --- | --- |
| Number | Title |
| 1 | Motivation |
| 2 | Description of the project   1. Background and related work 2. Project goals, expected outcomes |
| 3 | Methodology   1. Proposed ideas, methods, algorithms |
| 4 | Design and implementation   1. Design, implementation diagrams (with the tools used) |
| 5 | Testing and evaluation   1. Testing scenario required with the results (with the tools used) |
| 6 | Milestone, roles/tasks assignment |
| 7 | Conclusions |
| 8 | References |

1. **Motivation**

Medical records are crucial to maintain and keep secret to the world. In the USA, health care policies are wide to understand and hence it is pretty hard to implement the application to match the level of the HIPAA. Every day lots of private data are produced in different organization and send it to different location. Administrative policies are unique to each different type of data. Data needs to keep secret for client’s privacy as it transfers over the air or wire medium. HIPAA was passed in 1996 by U. S. Congress and stands for Health Insurance Portability and Accountability Act. Access control model is needed to cultivate the HIPAA policy. There are some engineering procedures that we need follow to meet the standards.

There are mainly three objectives that we need to consider during developing the application finance information, insurance health care, and data privacy. There is a growing industry for keeping the general population’s health information secure. Obeying the HIPAA (Health Insurance Portability and Accountability Act) Privacy Rule, many companies are making significant sums of money keeping health care information secure. The HIPAA Privacy rule enforces several mandates, the two of the most important being that appropriate safeguards must be in place and patients can control certain uses of their information.

1. **Description of the project**

**Background and related work**

HIPAA was introduced by congress in 1996. The major concern to use HIPPA is to provide vital health insurance record among the all users. The Health Insurance Portability and Accountability Act is developed to ensure the security and privacy to the patients records. HIPAA is mainly concentrate on electronic data transfer over the different locations in the world with secure mechanism. The HIPPA is introduced to the following standards such as transaction of information with sets of codes, identifier, privacy and the security. The people who are using health plan are automatically included in this feature. There main three areas where the HIPAA is concentrating now - Health plan, Health ClearingHouse and Health provider.

The standard transaction between third party (insurance agent) and user (Patient) are related to each other, where they can share the electronic information. The EDI (Electronic Data Interchange) is the procedure that provides standard of data documentation over the given of the information with security. The major tools are providing for finance health care administration for the HIPAA eligibility, Health care policy, Report of injury, Payment plans, HIPPA benefits etc. There are various applications are available in the market but they are really expensive to use. The HIPAA consist names, DOB, insurance number, address, phone number, license number, social security number, Vehicle identification number and biometric information.

There are several HIPAA compliance tools available in markets but they are associated with the specific associates. Like Management tools, business tools, Risk assessment tool and Rapid-fire tool, Sophos Encryption system tool. Every tool has their own mechanism and independent functionality but they are limited to the world in terms of attention to data security as a whole. These tools are to identify the particular parties with best HIPAA protocol practices. Depending on the different types of breaches, the tool monitors the activities and prevents the threat. Technical assistant keep eyes on this kind of issues and work under vulnerabilities. The best practice on this tool is to consider the following factors.

1] Process – Identify the needs and audit the process.

2] People – Medical testing, Background verification, insurance policy review and HIPAA healthcare protocols for people.

3] Tool – Restriction module, Access control methods, restricted access policy views.

All these tools are defined privacy protocol, Access protocol, Audit rules, and Security protocols. Depending on the health care provider such as Doctors, Dentist, Pharmacies, clinics, psychologist and nursing homes works with different healthcare plans such as Health care companies, Govt. health plans, and private health sectors. All above parties are part of one tool that taking care of electronic data transfer and entity that carrying the information and with information structure shares among these parties.

**Project goals, expected outcomes**

Project goal is to develop the mobile application that provides flexible and cheap way to use of HIPAA standards for the users such as doctor, patient and insurance agent. DOMO should meet the HIPPA standard to provide the secure mechanism for the data over the medium. Project goal is to provide the fast and easy access to the medical information. The policy is to provide the health information made available to the authorized user.

Our project goals are

1. Strong user authentication
2. Valid database access to authorized user.
3. Backend encryption

Expected outcome is - user authentication using role based access and validation of the information and generate the proper outcome. User can access only required information over the given credentials provided according to the protocol standards. There are three main roles in the proposed application.

A. Doctor, B. Patient and C. Insurance Agent.

The doctor has all access levels in given application to read, write, and execute. Where patient can only read, and write the data/ information. The health insurance agent can only access the information to read the data.

1. **Methodology**

Existing methodology supports the limited functionality with third party role in given figure CIA module works for each different phase but given module is blind fall between two parties. Third party that takes care of this all transaction is more concern about the information. To make it available and visible to the main characters, we are developing one simulated tool that supports the crystal-clear data security and modular functionality. Privacy, security and breach notification are the most focused areas in proposed system.

In order to complete our project under our time limitations, we chose to use the waterfall design model for planning and executing our software development lifecycle. Due to the relatively large scale and scope of our project, we found that the waterfall model would be most appropriate so that we could develop each stage incrementally on a timetable and accomplish each step according to schedule.

The stages of the waterfall model include the requirements gathering phase, the logical and physical design phase, the implementation and unit testing phase, the integration and verification phase, and finally the deployment phase. Figure 1 shows the various steps of the design model applied to our project. In the following sections, we cover each stage in the design model in detail and describe how we implemented each step accordingly.

1. *Requirements*

Currently, there is a crucial need for better security mechanisms implemented in HIPAA domo applications. Existing HIPAA applications are available through mobile markets are strikingly inadequate; almost all of the applications available do not implement any sort of less implementation cost and easy accessibility to the private data.

The couple that do, perform high performance and have high cost of implementation rates. Our three-pronged approach to developing a more secure HIPAA “DOMO” solution, includes improved user validation, secure data access and safe data encryption. In this section, we briefly discuss each part, then we describe the system requirements that we determined based on our desire to incorporate these three concepts.

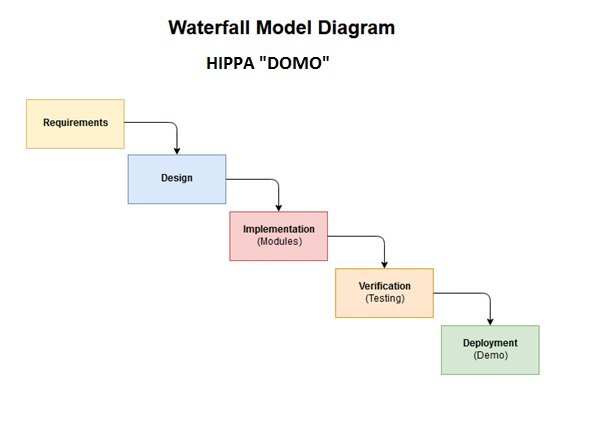


Fig. 1 The waterfall design model for HIPAA “DOMO” lifecycle

1. *Design / Proposed Idea*

In our proposed system, we are trying to generate the application design structure. It goes through the certain stages such as

1. Doctor – Update/View and Refer
2. Patient – View and Accept or refuse the referal
3. Insurance agent – Provide the claim for the patient’s or doctor’s request.

Encryption and decryption of the data/information over the online database server. Easy front end access that ask for user credentials to provide self authentication.



Fig.2 The design structure for HIPAA “DOMO” lifecycle

1. *Implementation / Methods*

The third stage of the waterfall design model of the implementation stage. All of the GUI design features are implemented in Android Studio for each of the activity windows. Activities are the terminology used in Android to describe an application frame or window. In this stage, we design the various activity windows and implement the program logic using the Java language.

The various modules that we have designed for the implementation domain of our project are coded in this stage. These include the user validation, Role based access, and data encryption.

We are using RSA encryption decryption algorithm for the data that we are storing in the database. We are using generation of public key, private key, encryption method and then decryption method of the data.

We have developed the login credentials to add the user login with user name and password.

RSAEncryptionDecryptionUtil

public PrivateKey getPrivateKey

public PublicKey getPublicKey

public String encryptText

public String decryptText

public class PasswordEncoderUtil

RSA algorithm: Rivest-Shamir-Adleman algorithm is developed in 1977 and used for data cryptographic public key encryption. It is used to send the data over the unsecured network. It is also known as public key cryptography or asymmetric cryptography. Two different but inter linked keys are used to communicate. One is public key is open to communicate and private key is used to private encryption. RSA support the SSL/TLS and digital signature. RSA keys are 1024 bits long.

1. *Verification*

In this stage of the waterfall model we integrated all of the modules together into the system. We then tested and verified the application’s functionality as a whole and debugged any problems that surfaced. This was the final stage of implementation and testing before we were ready for the last stage of deployment.

1. *Deployment*

This stage of the waterfall model is the final stage where we prepared for the deployment of our application. We prepared our final documentation and designed a presentation to demonstrate the application. This stage represents the completion stage of the waterfall model.

1. **Design and implementation**

In this phase, we have used the Amazon Wen Services (AWS), XAMPP for the database creation Bitnami for database connection. It consists direct interaction among the patient doctor and insurance agent straight through the application. Our goal is to provide the flexible integration and interaction among main parties rather than control by third party tool. Our main motivation for this project is to provide the secure virtual storage to the interconnected world, flexible and secure services, and most important is to make this application cheaper in costs that deserve/need this service.

Design phase will be developed using waterfall model and software tools are as follows

* + Android Studio
  + Amazon web services
  + XAMPP database
  + Bitnami connection from AWS to XAMPP
  + java
  + RSA

Android studio is to develop and simulate the application for the testing the virtual environment for the given application. In android studio, by our project, we can connect the front end with back end using PHP. Front end will be the java code that connected with some events on the key press button on the GUI.

Amazon Web Services are the services that used for online storage creation for the free database events. AWS is the runtime environment that updates the queries over the internet in dynamic environment. The process itself is lengthy but you can use the data encryption method. AWS is the best and fast reliable resources where you can store the data and retrieve the data dynamically.

XAMPP database is used to store the encrypted data over the given application where user gives the input data and it stores in backend with specified queries and retrieve it upon given request to fetch the data. In XAMPP we have created six tables, Doctor, Patient, Insurance Agent, Insurance details, Role based data. Each and individual table is join to one other and generate the information upon the query execution at the back end. XAMPP is cross platform web server and it is opensource to use. It supports PHP, MariaDB, Apache, and Perl. Cross platform means it support different operating systems such as Windows, Linux, and Mac.

Bitnami is the opensource source package installer for developing web based application.

It performs MySQL installation for the Apache with PHP MyAdmin. It provides automated deployment of sources for the online servers such as AWS, Goggle cloud server, and Oracle cloud server. There are various versions are available in the market according to the given platforms.

Java is used to create the front end with connection to online database. Java call the services that services are called in PHP file and PHP call the server for the given request and response. RSA is the combination over the system that implement the front end with system triggered events. RSA perform Key generation, Key distribution, Encryption and Decryption of the given message.

1. **Testing and evaluation**

AWS account creation and Bitnami connection

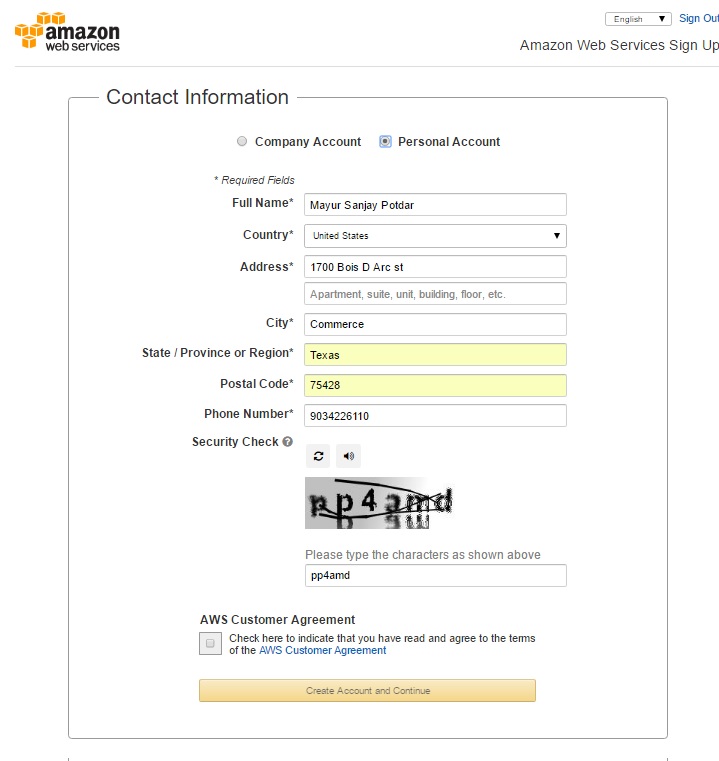


Fig. 3 AWS account creation

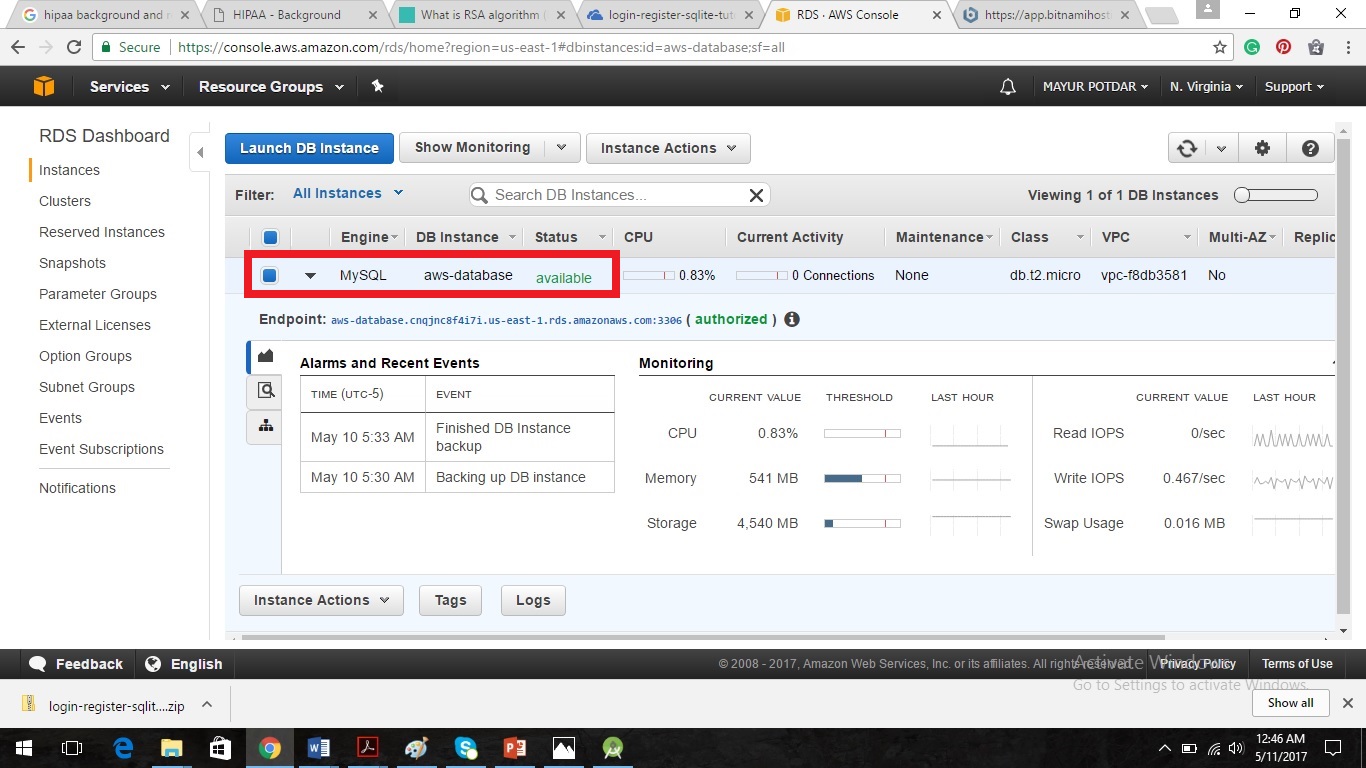


Fig. 4 RDS creation for the database

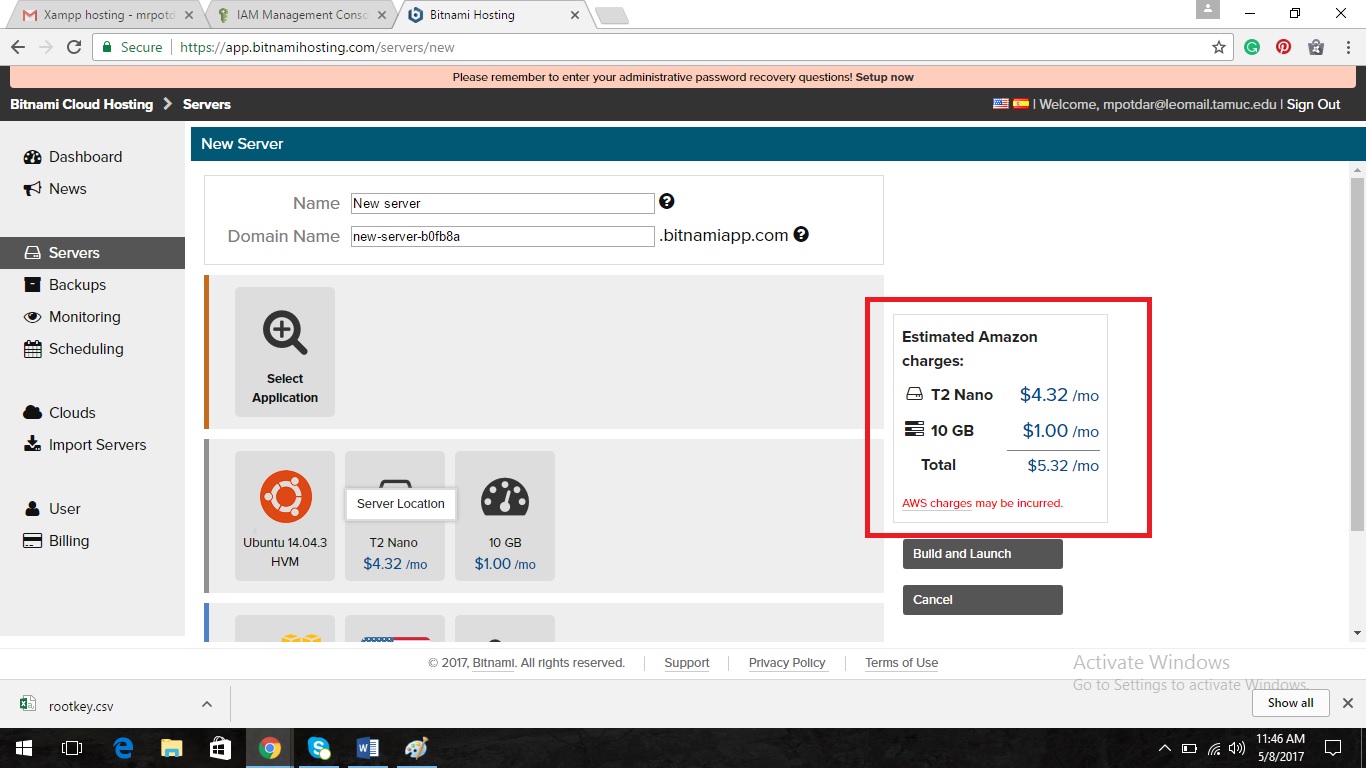


Fig. 5 Buying online space for the database

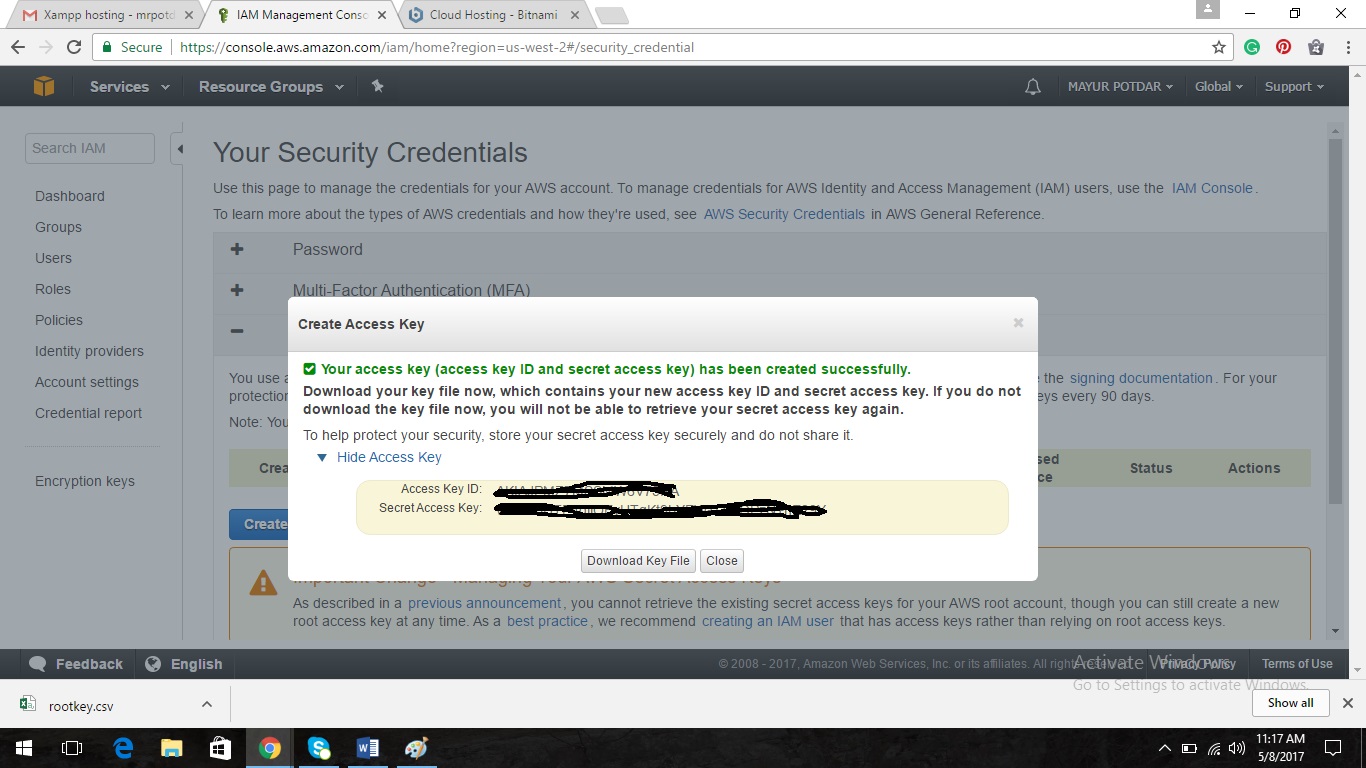


Fig. 6 Bitnami Key sharing for connection to AWS

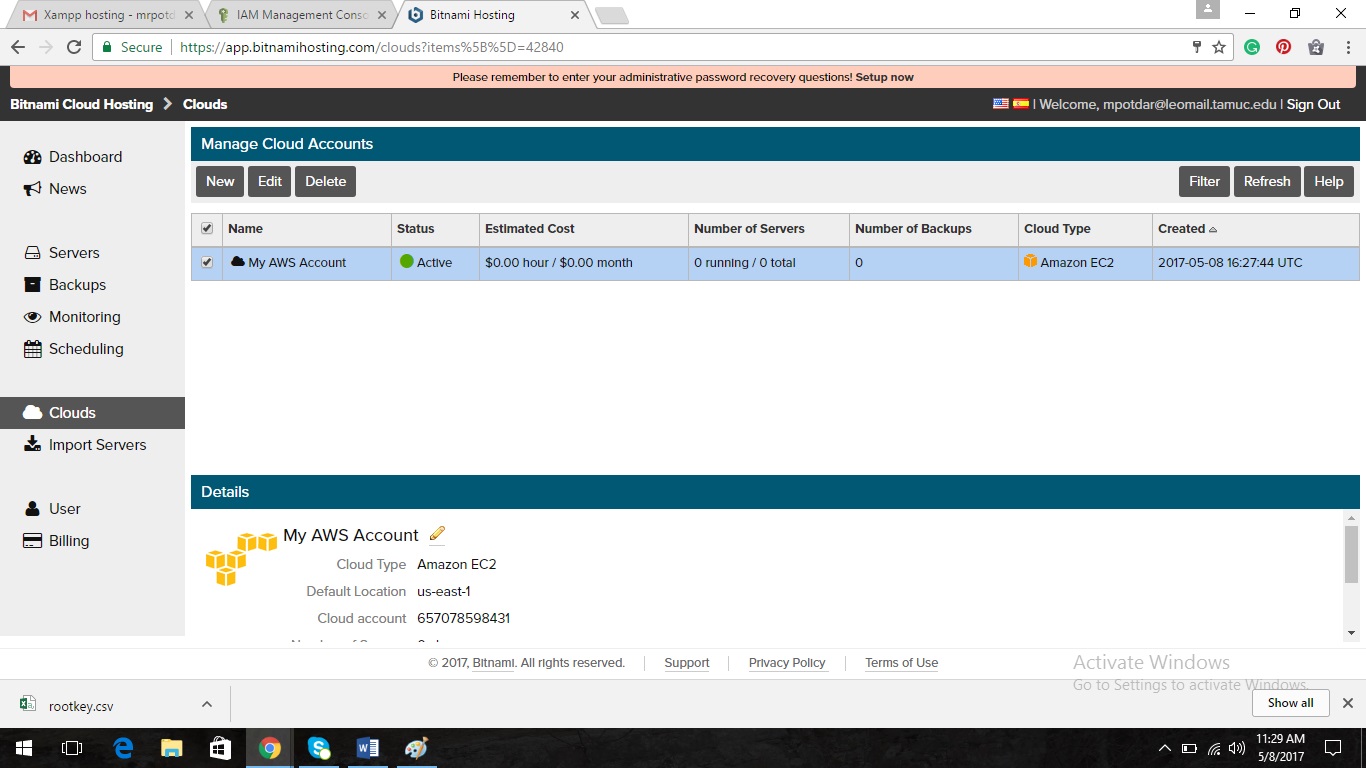


Fig.7 Bitnami AWS connection established

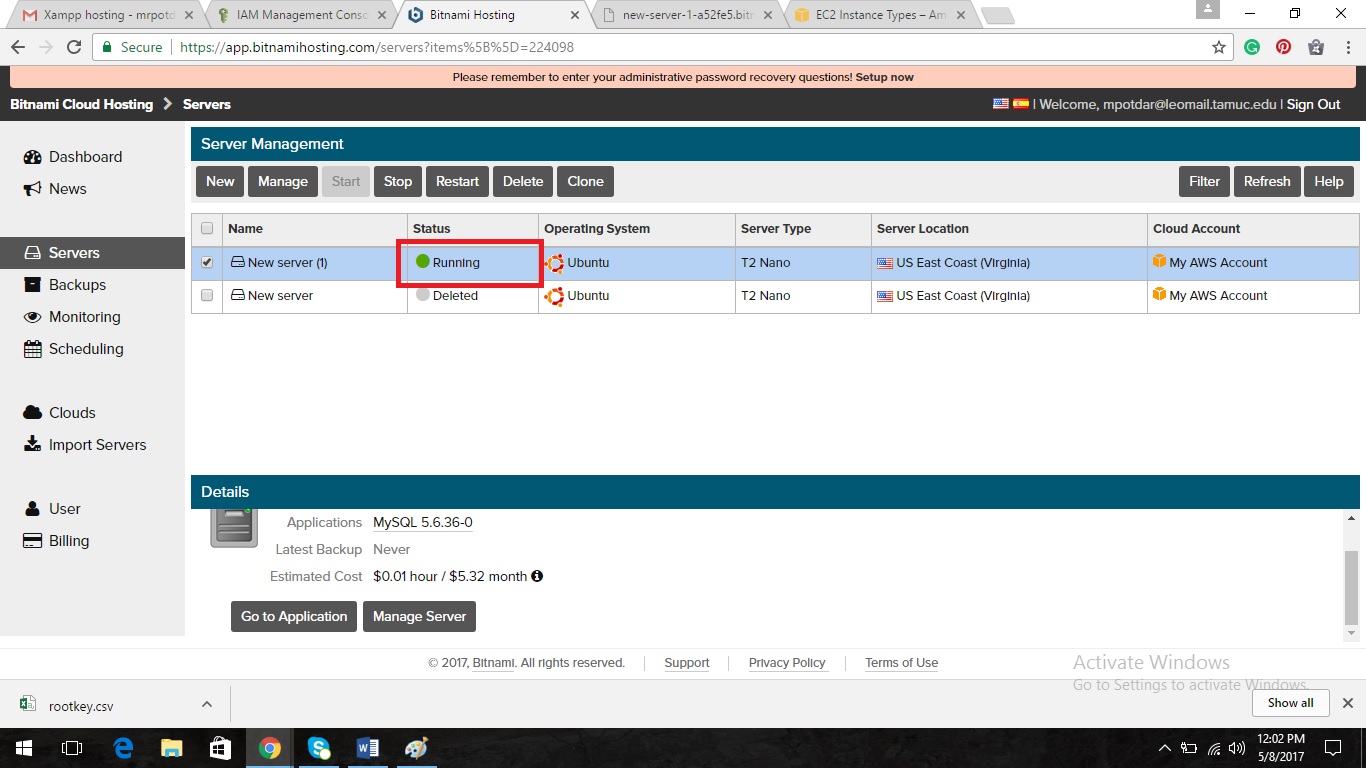


Fig. 8 Final connection to AWS and bitnami for hosting

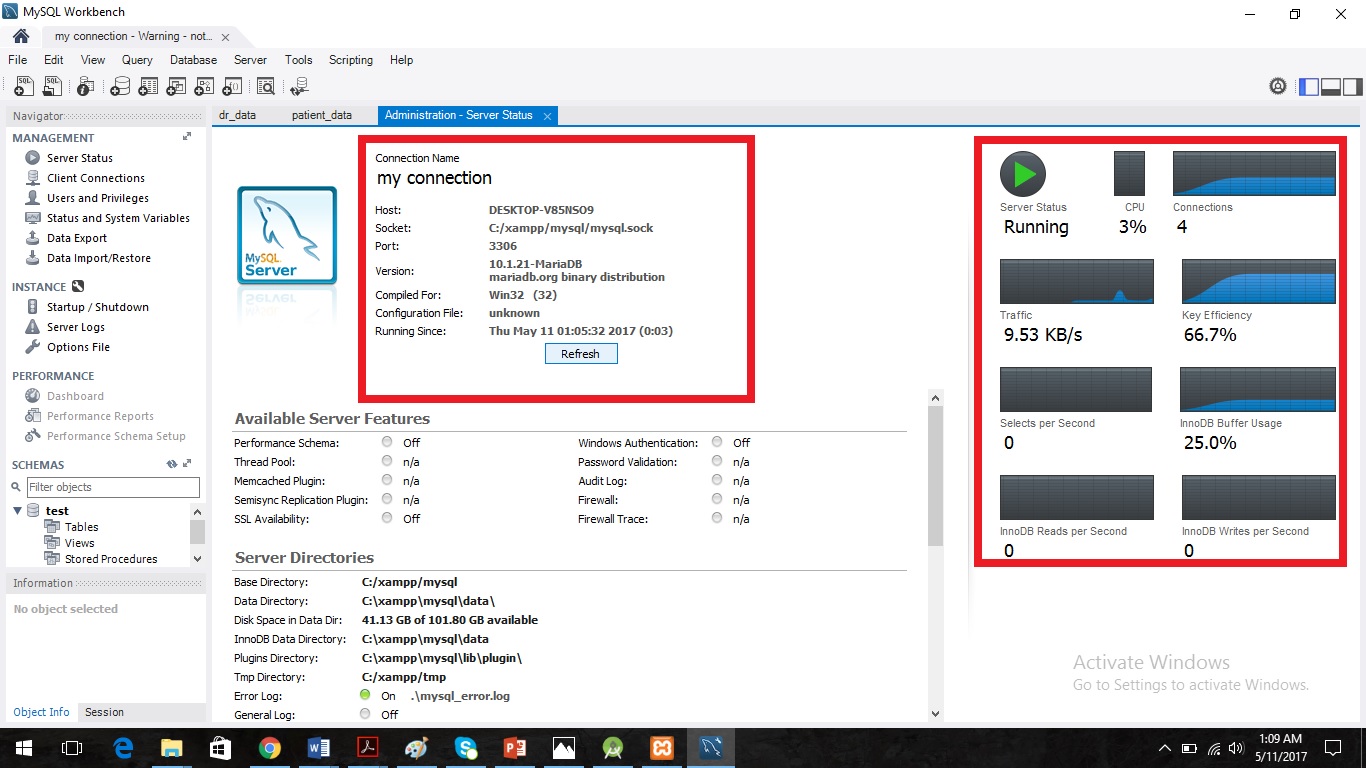
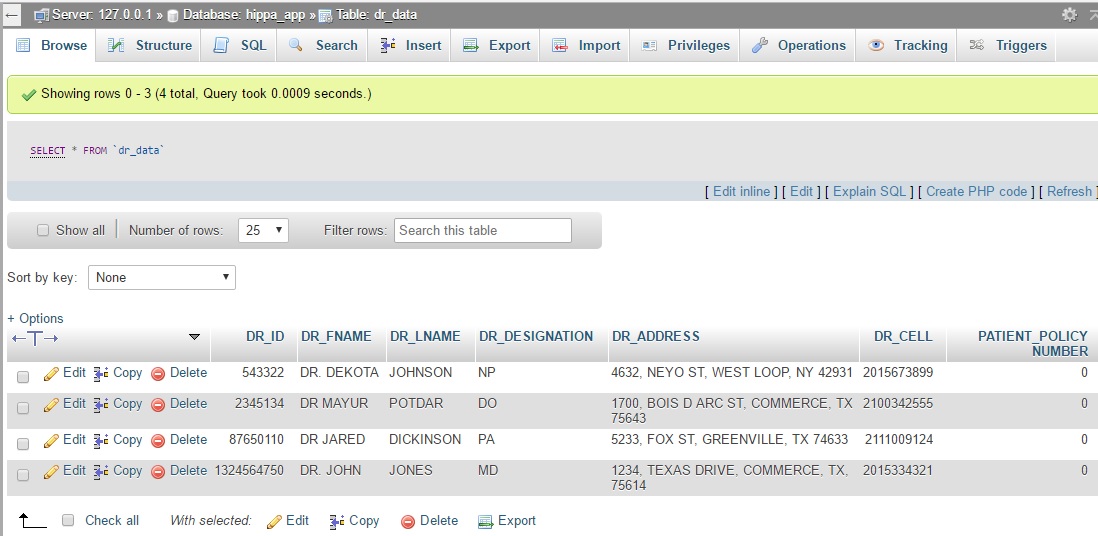
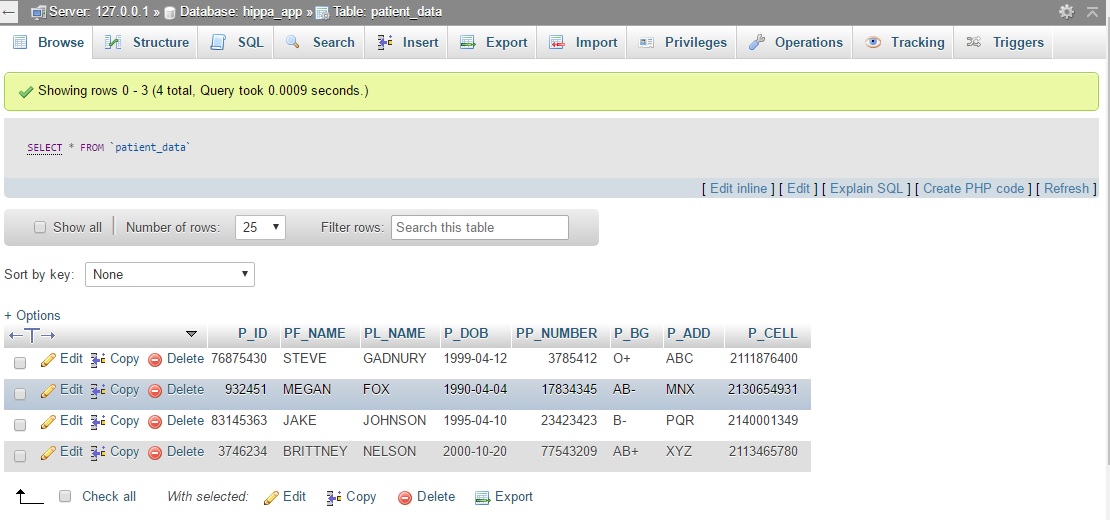
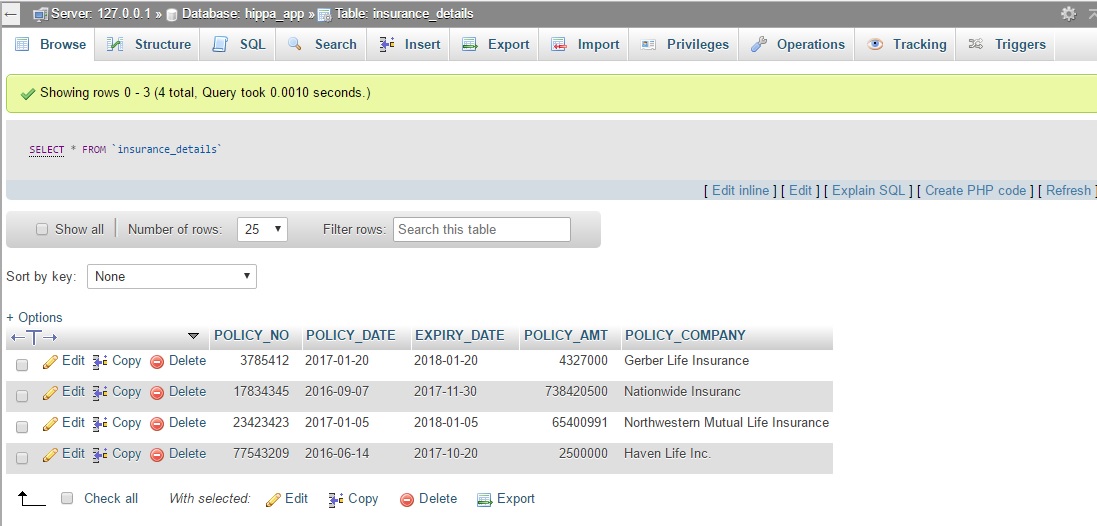
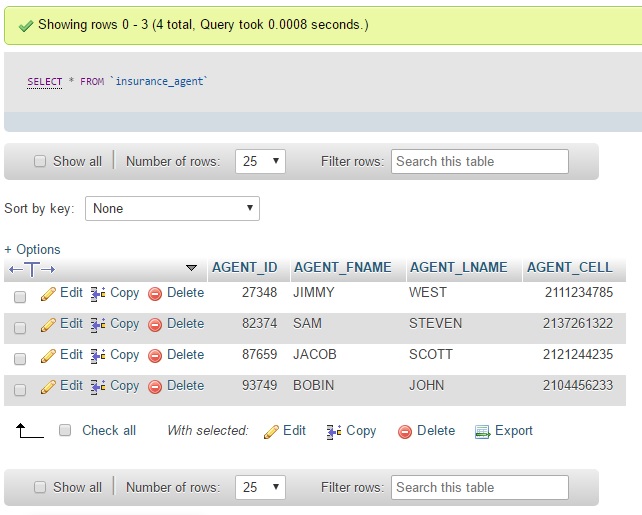


Fig.9 Database connection to workbench

Agent, Policy, Doctor and Patient database creation,



1. **Miles stones, Roles and Planning phase**

1. Planning:

Step 1: System and society requirements and define the modules.

Step 2: Develop each system module and create the database.

Step 3: Try to connect the interface between system and database using to test the environment.

Step 4: Develop the final project module

Step 5: Project demonstration with the final deployment.

2. Milestones:

Step 1: 1 week

Step 2: 4 weeks

Step 3: 2 weeks

Step 4: 1 week

Step 5: 1 week

3. Role/Task assignment

* Jared/Mayur – Research HIPAA standards
* Java code – Jared
* Mayur – implement online database
* Jared/Mayur – Database/App interface
* Mayur – Database Encryption
* Jared/Mayur - Testing

1. **Conclusions**

In this given proposal, we tried to develop the flexible application that reduce the gap between two parties and improve the qualities in the application that gives fast and flexible connection among all the modules. Even we are trying to reduce the price of implementation of proposed system that cost more than a million dollars in real market.

8. References

1] Tariq Alshugran; Julius Dichter **, “**Extracting and Modeling The Privacy Requirements from HIPAA for Healthcare Applications**”,** IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014, DOI: 10.1109

2] Denis Verdon and Gary Mcgraw “Risk Analysis in Software Design”, IEEE Journals & Magazines, 2004, pp. 79 - 84, DOI: 10.1109

3] Vivying S. Y. Cheng and, Patrick C. K. Hung “Towards an Integrated Privacy Framework for HIPAA-Compliant Web Services” Proc. E-Commerce Technology (CEC’05) 7th IEEE Int. Conf., 2005, pp. 480 - 483, DOI: 10.1109

4] Annie I. Anton, et al., “HIPAA’s Effect on Web Site Privacy Policies”, IEEE Security & Privacy **-** IEEE Journals & Magazines, Vol. 5, 2007, pp.45 - 52, DOI: 10.1109

5] Aaron K. Massey, et al., “Evaluating Legal Implementation Readiness Decision-Making”, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, 2014, pp. 545 - 564, DOI: 10.1109

6] <https://console.aws.amazon.com/console/home?region=us-east-1>

7] <https://app.bitnamihosting.com/servers>

8] <http://localhost/phpmyadmin/>

x. Final presentation – Jared and Mayur

**Conclusion:**

**References:**