**MEDICAL DATABASE SECURITY**

Submitted in fulfilment for

INFORMATION SECURITY SYTEM

BY

V RITHIK

UNDER THE GUIDANCE OF

**PROF. RAJESH KUMAR**

SECURITY PROBLEM:

The basic need of this system is now a days data has been undergoing attacks and also number of attackers are developing to get the data for making money and many other purposes and also the attacking techniques have been improvised medical information is 10 times more useful than credit card details on black market. Attackers discovers more methods so health care becoming a target because it contains personal data like contact number, address. So there is a need of protection for that patient data so in this project we are protecting the patient data not only from outside but also from inside .

The medical database security is a system that aims to provide internal and external communication among healthcare providers. Medical Database Systems provide a common source of information about a patient’s health history. The system has to keep data in a secure place and control who can reach the data in certain circumstances.

These systems enhance the ability of healthcare professionals to coordinate care by providing a patient’s health information and visit history at the place and time that it is needed.

Solution:

We can solve this problem by using front end and back end solution where it will be two way type communication, so it the front end does it work as it act like User Interface, which will be on our screen, as easy user interface "Front-end" typically means the parts of the project a user interacts with--such as the graphical user interface or command line.

The top most visible layer is what’s called the Frontend. This is usually written in java using NetBeans IDE.

And on the other hand it is about the database which is highly secured and keeps every information, records of the patients and others which helps the front end to work properly "Back-end" . It is also done by using java by connecting JDBC to it which provides security to our system.

This system code is done by using Java in Netbeans IDE applying HMAC algorithm and SHAmethods. Which will be very protected and safe for the system so the attackers cannot access easily into the database.

THE SYSTEM DESIGN ARCHITECTURE:



Elgamal Encryption

Upload

Paillier Decryption

**Server 3**

Paillier Encryption

Elgamal Decryption

**Server 2**

**Sensor Nodes**

**Doctor**

**Server 1**

CONCLUSION:

To keep the privacy of the patient data, proposed a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively. As long as one data server is not compromised, the privacy of the patient data can be preserved. For the legitimate user (e.g., physician) to access the patient data, proposed an access control protocol, where three data servers cooperate to provide the user with the patient data, but do not know what it is. For the legitimate user (e.g., medical researcher) to perform statistical analysis on the patient data, proposed some new protocols for average, correlation, variance and regression analysis, where the three data servers cooperate to process the patient data without disclosing the patient privacy and then provide the user with the statistical analysis results. Security and privacy analysis has shown that protocols are secure against both outside and inside attacks as long as one data server is not compromised. Performance analysis has shown that our protocols are practical as well. Unlike, the solution can preserve the patient data privacy as long as one of three data server is not compromised.

REFERENCE LINK:

<https://www.hindawi.com/journals/wcmc/2019/1927495/>

WHAT WILL BE YOUR NEXT PAPER:

1. IMPLEMENTATION.