www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 11 Nov 2015, Page No. 15020-15023

Secure data management system for patients and their doctor.

Miss.Revati Wahul[1], Miss.Eshaa Sood[2], Miss.Julie Yohannan[3], Miss.Zahra Budhwani[4]

[1]Assistant Professor Dept of Computer Engineer Mescoe Pune-01.
[2] Department of Computer Engineer Mescoe, Pune-01
[3] Department Of Computer Engineer Mescoe,Pune-01
[4] Department of Computer Engineer Mescoe,Pune-01.

Abstract: Database has been considered to be very important since a really long time and securing it now is of utmost importance-healthcare systems is very popular now but faces security constraints. The distributed m-healthcare systems allow significant patient treatment for medical consultation by sharing personal health information among healthcare providers. The important challenge is to ensure the security of the patient's identity as well as the data. Patients can decide which physician can access their information by using threshold predicates. Based on this idea we are devising a new technique where the patient can self-control their data with different ways of security. The directly authorized physicians and the patient can respectively decipher the personal health information and/or verify and update patient's health information at the click of a button.

Keywords: Database, Authentication, Security, Privacy, distributed system and healthcare.

1. INTRODUCTION :

We live in an information age where data should be accessible at the click of a button as well as data should be secured and not tampered with. Hence improving the security of database and medical data is the prime scope. Moreover medical data can now be available at the click of a button. We need to develop a system where all of the patient's health information is stored in a secured database, within a cloud. This data will be available only to the patient, his/her specific physician and the consultant(if there is one).Unlike most prior works, the new scheme further supports secure and efficient data transfer and data retrieval, with only user and his/her specified physicians and consultants able to access the given data. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient, malicious data modification attack, and even server colluding attacks, with backup available at all the time.

The given project is meant for easy access to patients who can access their records from everywhere and at the same time limit the people who can access their files. This document is intended to be read by the developers, users, testers, and documentation writers. This is a technical document and the terms should be understood by all of them.

2. Related Work :

In [1] author says that Database security is very important in today's world and it has received a great deal of attention since a very long time starting from data security for System R and Ingres to access control models to multilevel database systems. In[2] the author mentions that over the years various encryption schemes have been developed in order to protect the databases.

The paper discuss the importance of database encryption and makes an in depth review of various database encryption techniques and compares them on basis of their merits and demerits. In [3] the author has thrown light on how E-healthcare systems have been been popularised and is used in health condition monitoring, disease modelling early intervention, and evidence-based medical treatment by medical text mining and image feature extraction, but faces security and privacy issues. In the paper, a secure and efficient privacy-preserving dynamic medical text mining and image feature extraction scheme PPDM in cloud-assisted e-healthcare systems is proposed. In [4]the author through this paper is putting forward a novel authorized accessible privacy model (AAPM).Patients can authorize physicians by setting an access tree supporting flexible threshold predicates. Then based on it, by devising a new technique of attribute-based designated verifier signature, a patient self-controllable multi-level privacy-preserving cooperative authentication scheme (PSMPA) realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. The directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients' identities by satisfying the access tree with their own attribute sets.

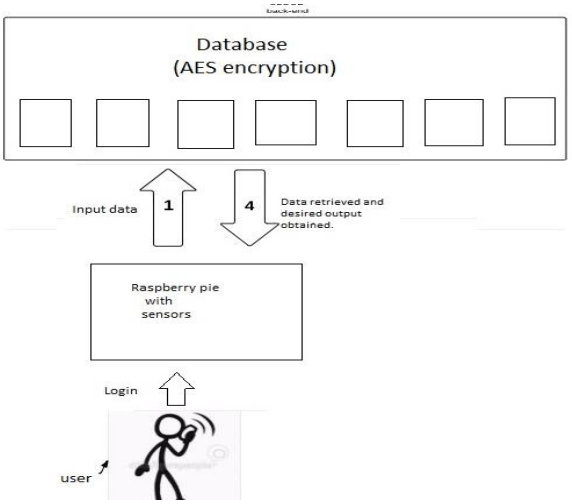
Modules:

- *Home Page*: Link to main page of user.
- *Sign Up:* Link to sign in for user.
- *Verification Details.*
- *File Display*: Medical data of the patient is displayed.

Home page: It will take the user to the system. Through this page user will have access to the system.

Sign in: There will be separate login for patient and doctor. Every patient and doctor will have their unique id and password.
Verification details: Proper authentication will take place both for the patient and doctor.
File display: After successful login and authentication the desired data will be displayed.

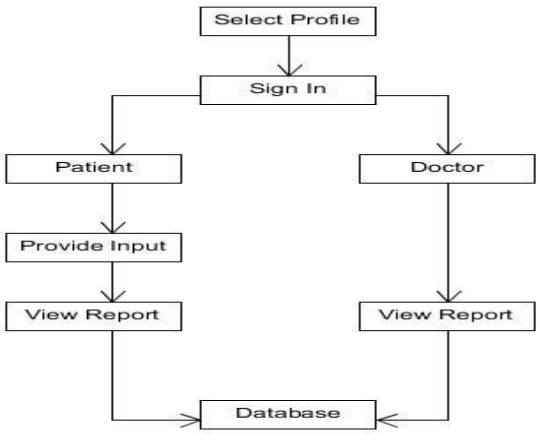
3. Architechture:



The user (patient/doctor) have to login through their specific user id and password.
After successful login patient inputs data through the hardware provided and data gets stored in the database
.Algorithm like AES is used to ensure its security.On request from user data is retrieved from database in a secured manner. The channel through which communication is taking place should also be sure by using hhtps to ensure that no data gets tampred during data flow also hence ensuring a complete secure system.

A. Data Flow Diagram:

DOI: 10.18535/Ijecs/v4i11.27



Description: Select Profile: There are options of either a doctor login or patient login.

Sign In:
Bothe the doctor and patient will have to sign in with a correct user id and password. Only after successful authentication can the sign in the system.

Patient:
a. The patient will provide input using the hardware and sensors.
b. She/he can view his/her record at the click of a button whenever needed.

Database: This is where the secure data is present. All requests are serviced from it.

Conclusion :

A system is developed where all of the patient's health information is stored in a secured database, within a cloud. This data will be available only to the patient, his/her specific physician at the click of a button. Unlike most prior works, the new scheme further supports secure and efficient data transfer

And data retrieval, with only user and his/her specified physicians and consultants able to access the given data. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient, malicious data modification attack, and even server colluding attacks, with backup available at all the time.

Acknowledgements:
We thereby thank our college MES College of Engineering (MESCOE, Pune for the motivation. Also we would like to thank our guide Prof. R.M. Wahul for her active support last but not the least

we would like to extend our sincere gratitude to our mentor Mr. Prashant Muley from Persistent systems for mentoring us throughout.

References:

[1] Thuraisingham. B, "Database security:past present and future", Big Data

(Big Data Congress), 2015 IEEE International Congress on June 27 2015-July 2 2015

[2] Markus Khne, Jrgen Sieck, "Database security using encryption", Second

International Conference on Artificial Intelligence, Modelling and Simulation,

November 2014

[3]Jun Zhou, Zhenfu Cao, Senior Member, IEEE Xiaolei Dong, Xiaodong Lin,

Senior Member, IEEE, "PPDM:Privac-Preserving Protocol for Dynamic Medical

test mining and image feature extraction from security data aggregation

in cloud-assisted e-healthcare systems",DOI: 10.1109/JSTSP.2015.2427113,

IEEE Journal of Selected Topics in Signal Processing

[4]Jun Zhou, Xiaodong Lin, Senior Member, IEEE, Xiaolei Dong, and Zhenfu

Cao, Senior Member, IEEE, "PSMPA: Patient Self-Controllable and Multi-

Level Privacy-Preserving Cooperative Authentication in Distributed m-Healthcare

Cloud Computing System",IEEE

Transactions on parallel and distributed systems, vol 26, No.6, June 2015

DOI: 10.18535/Ijecs/v4i11.27