Secure Sharing of Patient's Sensitive Information using Cloud Computing

Kiruthika. G
Computer Science & Engineering,
Sri Vidya College of Engineering &Technology,
Virudhunagar, India.

Bala Sugitha. G
Computer Science & Engineering,
Sri Vidya College of Engineering & Technology,
Virudhunagar, India.

Abstract:- **To maintain patient's sensitive health record in secure manner software is developed. Patient's information are stored in an online and retrieved for the purpose when needed. The software is very efficient but little bit lagging in security. Hence the software with security is developed, here for security reasons the patient's health and personal information's are encrypted and stored. If the information for the particular person is needed, the data are decrypted using a key and viewed by the doctors. For encryption and decryption, Attribute Based encryption algorithms are used.**

Keywords - Random Key, Attribute Based Encryption, Advanced Encryption Standard, Cloud Computing.

INTRODUCTION

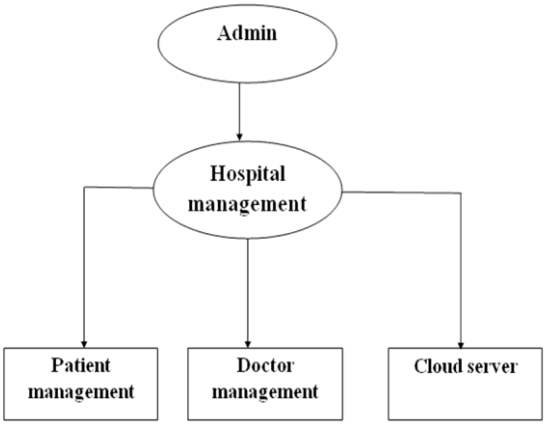
In the present day, patient's sensitive information maintaining is a major problems. A personal health record is an application used to maintain and manage patient's health information in a private, secure, and confidential environment. This stands in contrast to more widely used medical record, which is operated by institutions. The intention of a patient's sensitive information is to provide a complete and accurate summary of an individual's medical history which is accessible online. Most people do not carry medical records when they leave home. They do not think that in an emergency, which no one can predict, these medical records can make a big difference. In fact, they could save a life. Previous medications, history of allergy to medications, and other significant medical or surgical history are maintained in the software.

The main aim of the project is to hide patient sensitive information's against hackers and medicine companies. In this project admin manage patient, doctor module also Patient's Sensitive information's. The Patient health information's are encrypted using Attribute based encryption and upload it into the cloud. If the doctor wants to view the patient sensitive information, then they will send access request to the admin. Admin will send a secret key to the doctor email id, doctor need to provide this same id in the validate text box. Admin will redirect the download page if the key is correct, otherwise he can't. The doctor easily download the patient information, but could not read patient's details, only using encryption key he should be decrypt the patient information for understand about patient condition.

RELATED WORKS

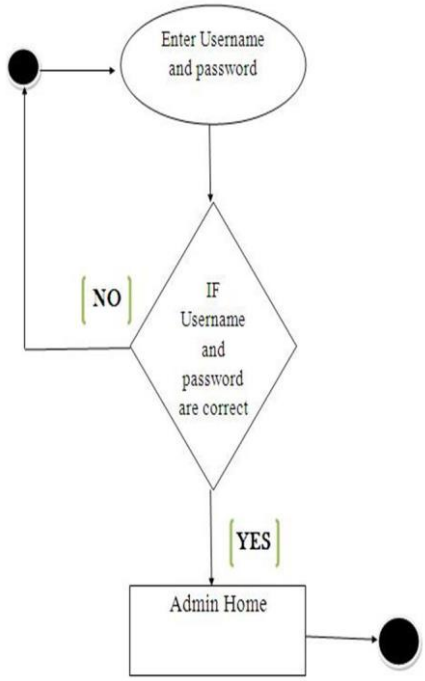
[1] The patients details are shared and maintained by their own the patients themselves. Using the properties of patient's personal information's, details are encrypted and stored in cloud. [2]In this paper encryption algorithms have been proposed to make cloud data secure, vulnerable and gave concern to security issues, challenges.[3]safe data retrieval mechanism is proposed and validated for retrieving personal health records stored in cloud in a hospital scenario.[4] In this paper the algorithms to encrypt and enhance data I cloud computing for security. [5] Efficient data encryption and decryption algorithms are used to protect an outsourced data. [6] In this paper explains the securities of cloud computing and encryption algorithms. [7] In this the basic concepts of cloud and how the data to be stored in cloud are explained. [8] In this the basic ideas of security algorithms such as RSA, DSA, Ceaser cipher are explained and how they are working. [9] This paper explains how the security algorithms are used in cloud computing. [10] In this paper using security algorithms how the data are stored in a security manner in cloud. [11] The basics of Cloud computing are explained in this paper. [12] In this paper how the security of cloud is maintained by HASBE and Hybrid Encryption Scheme. [13] In this paper Multi-authority attribute-based encryption enables a more realistic deployment of attribute-based access control, such that different authorities are responsible for issuing different sets of attributes. [14] Attribute-based cryptographic primitives provides flexible policies which can be used to build secure infrastructure for designing privacy preserving electronic health record system. [15] In this paper the attribute based encryption are used for to encrypt data and stored in cloud.

METHODOLOGIES



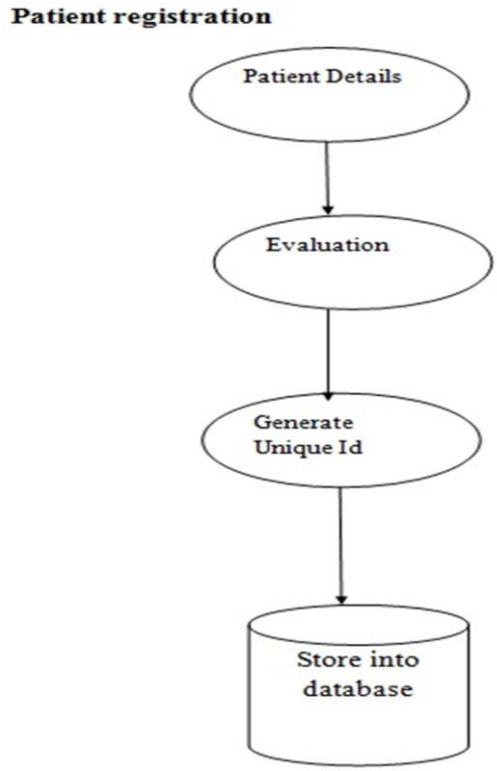
- Admin Management.
- Doctor Management.
- Cloud server module.
- Data confidentiality Module

The main goal of our framework is to provide secure patient's sensitive information access and efficient key management at the same time. The key idea is to divide the system into multiple security domains according to the different users' data access requirements. The public domains consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. Admin can enter into the software using a correct identity number and password. If correct, they can be admitted otherwise not.



In this module, admin plays a major role. Only admin have full rights to enter and modify details of the patients. And they also have rights to managing the doctor's details.

Each doctor has their unique id and password for access the cloud database in the hospital firm. The doctors also can view the patient details. The admin only upload the information of the patient. The doctor can enter using their id and password by sending a request to an admin. The random key will send to the doctor's mail id and the doctor have to see and enter that key then the doctor can enter into their login. Through mail the encryption key also send to the doctors.



The doctor can change their personal details but not able to change patient's details. When the doctor wants to view the patient details they have to enter the encryption key that sent to mail id only after the patient's sensitive information are decrypted. Finally, doctor can view the patients personal and health records.

In this module the patient information are stored into cloud database. That means the server will try to find out as much secret information in the stored Patient's health record files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

The admin upload Attribute Based Encrypted Patient's health record files to the cloud server. Patients record file is encrypted using Attribute based Encryption Algorithm. Only authorized users can decrypt the

health files, excluding the server. The users need to request a key for download the patient details. Then admin send it to the doctors personal email id. The doctors are should have submit the key. If the key is correct the patient' health details are automatically downloaded, otherwise it won't. The merits of the proposed system are the following:

1. The system can be used to maintain patient's details in a secured manner.
2. No one can easily retrieve or steal patient's personal health details.
3. Saves time and reduces human intervention.
4. Random key generation is another security in doctor's login
5. It makes doctors easily to view the patient's details.
6. The system is flexible and secured to be used.

RESULT AND CONCLUSION

We have developed Secure sharing of patient sensitive information using Cloud Computing. This system extremely user friendly. The system is tested with real data. The system is flexible so that there is a lot of scope to update the system. The developed system portable has been completed which is customized for the satisfaction of the user. The system has been analyzed, designed and developed with full care and can be executed without any faults or errors. As the system is flexible the system can be changed any changes comes in future.

ACKNOWLEDGEMENT

First and foremost, I would like to thank Almighty God for showing his blessing throughout our life. I take the privilege to express hearty thanks to my parents for their valuable support and effort to complete this project.

Our sincere thanks and profound sense of gratitude goes to our respected founded **Er.R.ThiruvengadaRamanuja Doss, B.E.,** for all his efforts and Administration in educating us in his premiere institution.

I take this chance to express my deep sense of gratitude to our dynamic Principal **Dr.S.Sangaralingam, M.E.,Ph.D.,** for providing an excellent infrastructure and support to pursue project work at our college.

My sincere thanks go to our project coordinator **Mr.K.Palraj, M.E.,** Assistant Professor, Department of Computer Science and Engineering towards his valuable support for our project.

I extremely happy for expressing our heartfelt gratitude to our Head of the Department **Mr.P.Murugeswari, M.Tech., Ph.D.,** for his technical support during the course of project. I extend my sincere thanks to my project guide **Mr.S.Gururagavendran, M.Tech.,** Assistant Professor, for his valuable guidance at each and every stage of the project, which helped a lot in successful completion of this project.

I am very much grateful to all staff members who helped a lot to complete the project.

REFERENCES:

[1] Ming Li,Shucheng Yu, Yao Zheng, 2012, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption".
[2] RachnaArora, AnshuParashar, 2013, "Secure User Data in Cloud Computing Using Encryption Algorithms".
[3] V.M.Prabhakaran, S.Balamurugan, S.Charanyaa, 2014, "Safe Data Retrieval Mechanism for Retrieving Personal Health Records (PHRs) in Cloud".
[4] ManpreetKaur, Rajbir Singh, 2013, "Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing".
[5] Prakash G, Dr. Manish Prateek,Dr. Inder Singh, 2014, "Data Encryption and Decryption Algorithms using Key Rotations for Data Security in Cloud System".
[6] VarshaAlangar, 2013, "Cloud Computing Security and Encryption".
[7] Wikinvest, "Cloud computing".
[8] RandeepKaur, SupriyaKinger, 2014, "Analysis of Security Algorithms in Cloud Computing".
[9] Vijayapriya M, 2013, "Security Algorithm in Cloud Computing".
[10] MandeepKaur, Manish Mahajan, 2013, "Using Encryption Algorithms to enhance the Data Security in Cloud Computing".
[11] AlexaHuth, James Cebula, 2011, "The Basics of Cloud Computing".
[12] R.Sinduja, G.Sumathi, 2013, "Improving Cloud Security by Enhanced HASBE using Hybrid Encryption Scheme".
[13] M. Chase, S.S. Chow, 2009, "Improving Privacy and Security in MultiAuthority Attribute- Based Encryption".
[14] S. Narayan, M. Gagne´, and R. Safavi- Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure".
[15] VipulGoyal, OmkantPandey, AmitSahai and Brent Waters, 2006,"Attribute-Based Encryption for Fine- Grained Access Control of Encrypted Data".