AADHAR CARD BASED HEALTH RECORDS MONITORING SYSTEM

Mrs. R.Harini[1], Mr. V.Gnanasekar, M.E[2], Mrs. R.Dhanapriya M.E[3]

[1]Pursuing M.E CSE Branch, [2]Head of the Department of Computer Science and Engineering,[3]Assistant Professor dept. of Computer Science , Gojan school of Business and Technology, Redhills, Chennai.

---***---

Abstract-- *The widespread acceptance of cloud based services in the healthcare sector has resulted in cost effective and convenient exchange of Personal Health Records among several participating entities of the e-health systems. Storing the health information to cloud servers is susceptible to theft and calls for the development of methodologies to ensure the privacy of the HRS. Therefore we propose the methodology called AES algorithm for secure sharing records of the patients. The AES scheme ensure patient-centric access control of the patients records and ensure the privacy and confidentiality of the record. Encryption works by taking plain text and converting in to cipher text, which made up of seemingly random characters. Only those who have special key can decrypt it. AES uses special key encryption, which involves the uses of only one secret key to cipher and decipher information. It uses lengthy key sizes for advanced encryption. Performance evaluation regarding time consumption indicates that AES methodology has potential to be or secure sharing of the health records in the cloud.*

Key words - Access control, cloud computing, personal health record, Advanced Encryption Standard.

1. INTRODCTION

Cloud computing is on demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term generally used to describe datacenters available to many users over the internet. Large clouds, predominant today, often have function distributed over multiple from central servers. If the connection to the user is relatively close, it may be designated an edge server. Cloud has emerged as promising paradigm for computing and is drawing the attention for both academia and industry. It offers pervasive and on demand availability of various form of hardware, software, infrastructure and storage. Consequently, the cloud computing paradigm facilitates organization by retrieving them from the protracted job of infrastructure development and has encouraged them to trust on the third party information technology services. Additionally, the cloud computing model has demonstrated significant potential to increase coordination among several healthcare stake holder. And also to ensure continuous availability of health information, and scalability. Furthermore, the cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers. Therefore, the integration for mentioned entities results in the evolution of a cost effective and collaborative health ecosystem where the patients can easily create and manage their Personal Health Records(PHRs).

2. RELATED WORK

M. Li, S. Yu and his member [1] proposed , a technique storing PHRs in semi trusted servers using novel patient-centric framework for data access control. To achieve fine-grained and scalable data access control for PHRs, we use attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. A high degree of patient privacy is assured simultaneously by exploiting multi authority ABE. But problem with this scheme is, it also enables dynamic modification in file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. In [2] Stefan katzenbisser and his members proposed a technique based on distributed attribute based encryption, in this paper, the construction of DABE is, where the arbitrary members can present and maintain attributes and their corresponding keys. It consist of specified logical combination of attribute is used to encrypt the data under access policy, this kind of encrypted data can be decrypted easily by any user, using the set of attributes that fits the access policy. Ming lee and his members [3] proposed a technique ,problem of private keyword searches on encrypted health records, here user gets the query from locally trusted authorities. This document assure security and query privacy. Hoang and his members [4] worked on message encryption and authentication using AES algorithm, this work is done using 8-bit AES encryption core, this implementation shows that work consumes low power and high efficiency. Bethencort and his members [5] proposed patient controlled encryption , the patient can share their record their doctors and healthcare providers. The record of the patient is partitioned in to hierarchal format, and each part of the encrypted portion is matched with its own key. The patient has its own key and the remaining part of the key is kept for decryption process.

3 . PROPOSED WORK

The key idea is initially, through the admin process hospital registration is done only after getting license for the particular hospital. Then the doctors will get registered and patients also get registered using their unique id, here the unique id is created using their aadhar card number. The patient can also claim for the insurance if they need. The patient's general information profile can be seen only by doctors or by management member of the health care who are having patient ID. A patient's health record comprises different types of data related to various areas like, cardiology, oncology, etc. The data in each area can also be different types like lab reports, medical treatment, discharge summary and so on. Each of these files based on a particular attribute. The management member will upload these, files using AES method. Additionally, in this framework, the data in the database is also encrypted. So that even if the intruders get access to database, they cannot read the data in the database. The data can be read only by the authorized person in the framework like PHR owners, doctors. In this proposed system. Donors such as blood donors and organ donors can also register. All these details of the donors are accessed only by doctors. So, whenever the blood is required they can send message to the donors for blood and the organ based on the requirement.

4. SYTEM ARCHITECTURE

The key contribution of the proposed work is given below:

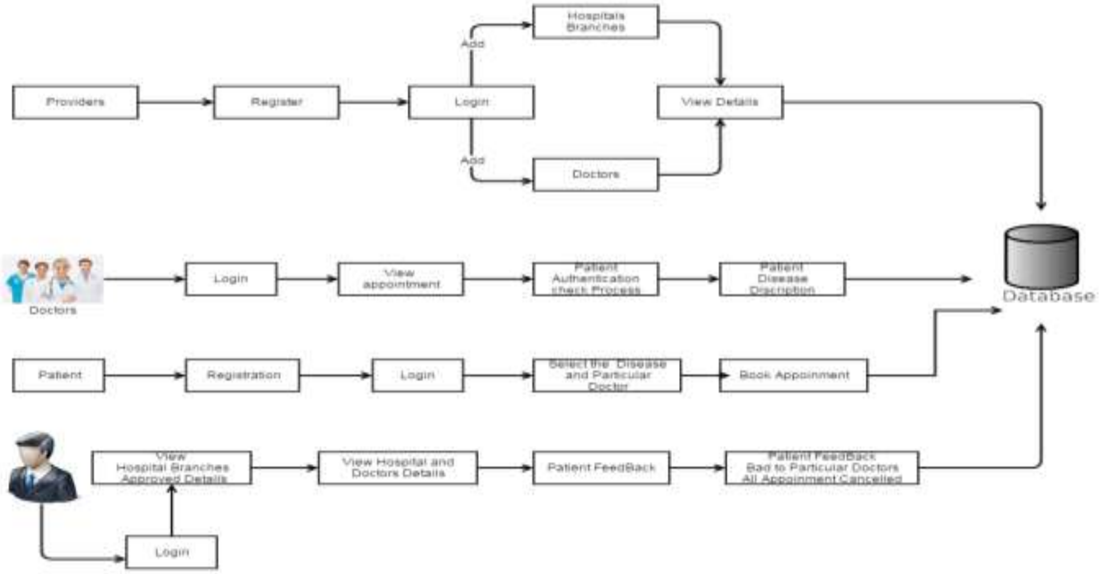
1. As it shown in proposed architecture diagram ,user will provide his/her basic details to the admin of the health care along with their aadhar number, so that unique id is created for the patient.

2. The user can login hospital website in order to view their profile, as well they can clear their medical queries with particular doctor etc.

3. The same way doctors can also visit hospital website in order to answer the queries of the patient and they can also view the appointments for them.

4. The records of the patient is stored in the database in the encrypted form.

5. When patient login to their profile, the records of the patients will be encrypted form, in order to decrypt the data user must access decrypt key to view correct record..


Providers
Register
Login
Add
Hospitals Branches
Add
Doctors
View Details
Database
Doctors
Login
View appointment
Patient Authentication check Process
Patient Disease Discription
Patient
Registration
Login
Select the Disease and Particular Doctor
Book Appoinment
View Hospital Branches Approved Details
View Hospital and Doctors Details
Patient FeedBack
Patient FeedBack Bad to Particular Doctors All Appoinment Cancelled
Login

5. PROPOSED MODULES

Admin Module

In the proposed work, an User must Authorised in an our application and there is a provider side must add the doctors and hospitals for the further counselling for Patients or Users... Even Doctor Profile, Doctors only able to known the Password for their view of Counselling Information..

Unique Id and Key verification

In this module, when an every provider must have an unique hospital details and doctor list.... When an User comes under in an application must have an unique id, to proceed next step, the process is verified.

Reports Upload

When an User booked his Provider along with Hospitality Functions and Doctor appointed in an application...Once an User come back for further Process They made an counselling to Particular Doctor.

Doctor Counseling

We consider the server to be semi-trusted, that means the server will try to find out as much secret information in the stored PHR 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.

User Entry Checking

In this Module, the main goal of the Project it denotes security for viewing our personal information to all roles in an application. To prevent that we had proposed to use Attribute Based Encryption Algorithm for the access to encrypt the Selected Detail Restrict to view by others.

Database Report Search

In this module, admin can able to view overall users report, Users personal Records and User Counselling Records in a encrypted form.

6. SECURITY

Encryption and decryption process:

Here, we restrict to description of a typical round of AES encryption. Each round comprises of four sub-processes. The round process is detailed below:

Byte Substitution (Sub Bytes)

The 16 input bytes are substituted by looking up are a fixed table (s-box) given design. The result is in a matrix of four rows and four columns.

Shift Rows

Each of the four of the matrix is shifted to the left. Any entities that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows-

- First is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

Mix Columns

Each columns of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16new bytes. It should be noted that this step is not performed in the last round.

Addround Key

The 16 bytes of the matrix are now considered as 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process:

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse- order

- Addround key
- Mix columns

- Shift rows
- Byte substitution

Since sub-processes in each round are in reverse manner, unlike for a feistel cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related

ADVANCED ENCRYPTIION STANDARD

To secure sensitive data, the advanced encryption standard method is used, in order to encrypt and decrypt the sensitive data. Based on its key length the number of rounds in the work, the encryption process is determined. For eg

- For AES-128 bit, 10 rounds
- For AES-192 bit, 12 rounds
- For AES-256 bit,14 rounds

IMPLEMENTATION OF AES

AES- 128, 192, 256 are bits process the data block in 10, 12, or 14 rounds respectively.

The data block is processed as follows:

- AES encryption starts by copying 16-byte input array using 4 by 4 matrix.
- The input data goes through first 128- bit of the cipher key.
- Resulting state passes through 10/12/14 rounds,and the output will be encrypted.

ALGORITHM

- **Key Expansion:** the chipper key and round keys are derived using key schedule of AES'
- **Initial Round:** each byte of the state is combined with the round key using bitwise XOR
- **Rounds**

1. **Sub bytes:** each byte is swapped with another in non-linear substitution method.
2. **Shift rows:** it's a transposition step, each row of the state is shifted cyclically.
3. **Mix columns:** mixing operation is done in the columns of the state, combining 4 bytes in the columns.

- **Final Round:** no mix columns

CONCLUSION

This paper discuss the two crucial aspects of PHRs one thing is security and data access control. Here data is arranged in attribute wise and data is secured using AES algorithm.

REFERENCES

[1] M. Li, S. Yu, Y. Zheng, K. Ren, (2013) "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems.

[2] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng (2012) "An smdpbased service model for interdomain resource allocation in mobile cloud networks," IEEE Transactions on Vehicular Technology.

[3] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, (2014) "Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and Health Informatic.

[4] Y. Yang, H. Li, L. Wenchao, H. Yang, and W. Mi, (2014) "Secure dynamic searchable symmetric encryption with constant document update cost," in Proceedings of GLOBECOM.

[5] Ernst, Young (2011) data loss prevention: Keeping your sensitive data out of the public domain. Ernst & young Global Limited, United Kingdom.

[6] Twum F, Nti k, Asante M (2016) Improving security levels in Automatic Teller Machines (ATM) using multifactor authentication. Int j sci Engg Appl 5:126-134.

[7] Tatum WM (2001) The Advanced Encryption System (AES) development effort: Overview and update.Sans Institute.

[8] Anitha P, palaniswamy V (2011) Data Protection Algorithm Using AES. Int J current Res33:291-294.

[9] Gayathri K, Yasmeen W (2014)Data encryption and decryption using AES with key length of 256 bits. Int J sci Engg Tech Res3: 4143-4146.

[10] Barrow M (2011) Patients get right to see the medical records online. The Times.

[11] Sultan N (2014) Making Use of Cloud computing for Health care Provision: Opportunities and Challenges. Int J Inform Manage 34:177-184.

[12] Aziz HA (2015) Health Informatics – Introduction. Clin Lab Sci 28: 238-239.