Secure Health Records Using Biocryptography

P.V.S. Chandana, P.S.G. Arunasri , D. Meenakshi , P. GopiKrishna

Abstract: ***Various works have proposed and executed cryptography as an approach to defend the insurance and security of the patient's restorative information. Electronic wellbeing record (EHR) is progressively actualized in numerous nations. The need for the EHR increases due to the quality of the medical care and it is also cost-effective. The use of Bio-cryptography is to secure medical records by m taking advantage of a fingerprint. As of the existed system contain different types of techniques using cryptographic algorithms and mobile Scenario's. In this paper, we proposed a system with the help of the web application using a fingerprint module and cryptographic algorithms. After successful registration of the patient record only the administrator, patient and the guardian can open the record using fingerprint and cryptographic algorithms. The authenticity and trustworthiness of the record will be secured using the security challenge questions which are inserted within the system.***

Index Terms**: EHR (Electronic Health Record), Bio-Cryptography, biometrics , authenticity.**

I. INTRODUCTION

1.1. Electronic Health Records

An electronic wellbeing record is an advanced form of the patient's restorative record. It has a patient's medicinal data like therapeutic history, analyze, prescriptions, treatment plans, vaccination dates, radiology pictures, x-beam, research centre and test outcomes. It will enable access to instruments which will utilize suppliers to settle on choices about a patient's consideration and keep up robotizes and streamline supplier work process. EHRs will examine the data with other social insurance suppliers and associations, for example, labs, pros, restorative imaging offices, crisis offices from all clinicians engaged with patient's consideration. When the patient's medical information is shared or communicated Without the patient's permission the patient can conceal the information due to lack of confidence in the security of the system having their information. In this express, their treatment might be compromised [2]. There is a risk of theft or any misstep can happen. The Health workforce and policy decision to implement the policies in the EHR and implemented the new tool like EMR which is likewise same as the EHR but it provides the new suppliers and functionalities.

1.2. Potential Benefits

A medical record that was utilized before is of paper-based application documented for research, clinical, administrative and financial purposes. It is the main cause in terms of accessibility, and it will be visible to every user and the administrators which are unsecured and unauthorized. It will be expired within 6 months and also updated manually. The purpose of EHR documentation is to secure the records with all benefits that include human services by improving all parts of patient consideration, security, viability, persistent centeredness, correspondence, training, immortality, productivity, and value. EHR's have a few preferences over paper records. generation of advanced records diminishes numerous issues of wrong solutions, portions, and system .Therefore the adverse reactions that were done by the wrong medication or any expiry medication can be avoided and secured by connecting the drug banks and pharmacies to the EHR[2]. This should be possible by not allowing medicine and request for any medications for which an unfavourable response can happen for a specific patient. This is effectively available from anyplace inside less length which is advantageous to the patient .It also requires less space to store and cut the number of records with a replacement of papers and it will be very helpful while research activities. It can likewise be reinforcement records requiring little to no effort, speed information exchange, and furthermore practical. It is fundamentally used to lessen medicinal mistakes.

1.3. Privacy And Authenticity

The patient records are used to be very confidential and secured and it cannot be released to others without giving permission from the patient side or by the law.

Revised Manuscript Received on April 07, 2019.

P.V.S.Chandana, Department of ECM , Koneru Lakshmaih Educational Foundation , Vaddeswaram.

P.S.G.ArunaSri , Associate Professor, Department of ECM , Koneru Lakshmaih Educational Foundation , Vaddeswaram.

D. Meenakshi, Department of ECM , Koneru Lakshmaih Educational Foundation , Vaddeswaram.

P.Gopi Krishna , Assistant Professor, Department of ECM , Koneru Lakshmaih Educational Foundation , Vaddeswaram.

At the point when the patient is unfit to do in light of age, mental limit the decisions that cannot be taken by themselves can be cleared by using the legal representative or any legal guardian of the patient. The information that is shared between the persons can be protected and secured safely by the EHR.

The institutions which are linked together by the EHR will require the accessibility of the data to present in their own way. This includes the information must be secured in a confidential manner using a technique that allowing only the authorized users to have access to information. The client's approval will be based on the administrator identifies the user, determines the data need to be communicated with other health cares and also make sure to assign the username and password to the authorization. Although providing security measures the confidentiality is not sufficient to preserve the passwords. This paper deals with the strong security using the fingerprint modules. The information will be opened only when the user used his/her thumb to open the lock so it will be very confidential while using the EHR.

1.4. Security Issues

There are many security techniques like mobile platforms, EHR passwords, cryptographic algorithms using biometrics etc. There are so many issues regarding the safety of health data. This paper deals with the privacy and security of patient medical data which is highly secured using fingerprint and some cryptographic algorithms. The medical record will only be exposed to the user until and unless he/she scanned the finger in the scanner[2].

II. LITERATURE SURVEY

This paper[1] deals with a set of cryptographic algorithms to secure medical records in mobile platforms. The cryptographic calculations are utilized to keep up the records with the assistance of registering memory, preparing and time in each contemplated calculation. A system is developed with the help of algorithm which is compared in the basis of time, memory and the processing consumption. It is highly secured with mobile platforms by comparison of different Algorithms and justified the best algorithm.

This paper[2] manages Electronic wellbeing record (EHR). It is continuously being executed in many making locales in wherever all through the countries. It is the need since it improves the nature of human services and is additionally cost-effective. The reason for this paper is to diminish the dangers and conquer the dangers with computerized records. These can likewise be verified with the assistance of encryption of the record. The another verified system utilized in this paper is EMR which is more secure than EHR. EMR improves the quality, wellbeing, productivity, and adequacy of social insurance conveyance frameworks.

This paper [3] deals with cryptography and also some algorithms to preserve the security and privacy of the health records. It secures the medical records with the help of bio-cryptography. EHR' s are provided with security by taking advantage of fingerprint and iris features. These records are protected by fuzzy vault and fuzzy commitment algorithms. The feasibility of implementing a fuzzy key binding scheme in real applications, particularly fuzzy vault that incontestable an improved performance throughout key reconstruction. This outcome likewise legitimizes the practicality of executing a fluffy key restricting plan in genuine applications, particularly fluffy vault which showed a superior execution amid key reproduction.

III. THEORITICAL ANALYSIS

3.1. Bio-cryptography key binding approach

The keys generated were stored in user's biometric templates using different biometrics. The fingerprint minutiae and some cryptography algorithms are used to secure the data.

3.2 Fingerprint

The fingerprint minutiae served as the biometric templates, which were stored in the database in the form of cryptography data[3]. The main reason for the choice of this biometric in this Project are:

• It will take less time for enrollment

• More number of people is comfortable with identification based on the use of the fingerprint.

3.3 Flow charts

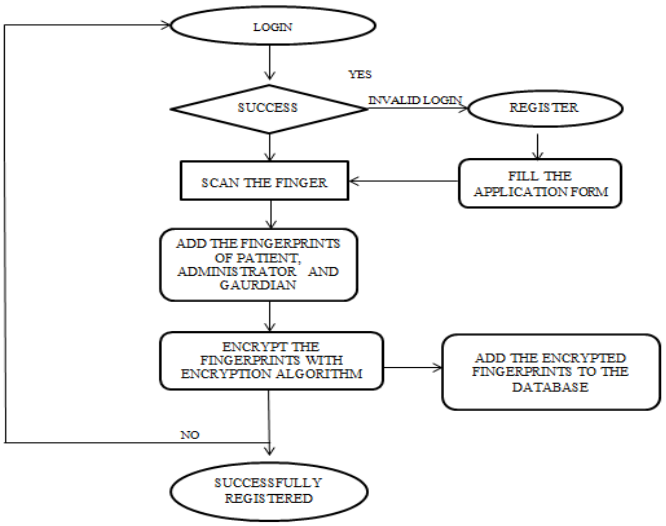

Fig 3.3.1.Block diagram for Registration

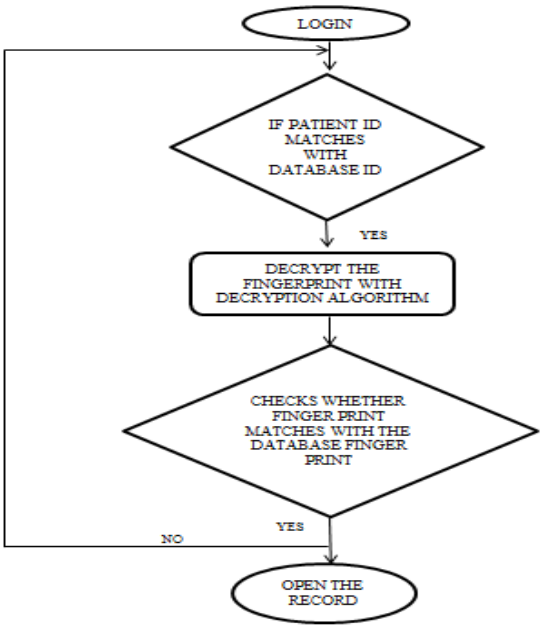

Fig 3.3.2.Block diagram for opening the record

3.4.Algoritms used

The Advanced secret writing customary (AES), additionally renowned by its original name Rijndael (Dutch pronunciation: could be a detail for the mystery composing of electronic data built up by the U.S.National Institute of Standards and Technology (NIST) in 2001.AES could be a set of the Rijndael block cipher developed by 2 Belgian cryptographers, Vincent Rijmen and Joan Daemen, World Health Organization submitted a proposal to authority throughout the AES choice method[8][9].

AES computation is of three sorts, for instance, AES-128, AES-192 and AES-256. This request is done on the bases of the key used in the figuring for encryption and unscrambling process. The numbers address the range of a key in bits. This key size chooses the security level as the proportion of key forms the component of security increases. The AES figuring uses a round work that is made out of four differing byte-orchestrated changes. For encryption reason, four rounds contain:

- Substitute byte
- Shift push
- Mix portions
- Add round key

While the unraveling technique is the pivot strategy of the encryption which involves:

- Inverse move push
- Inverse substitute byte
- Add round key
- Inverse mix areas

There is different round present of key and square in the estimation. The amount of rounds depends upon the length of the key use for Encryption and Decryption[10].

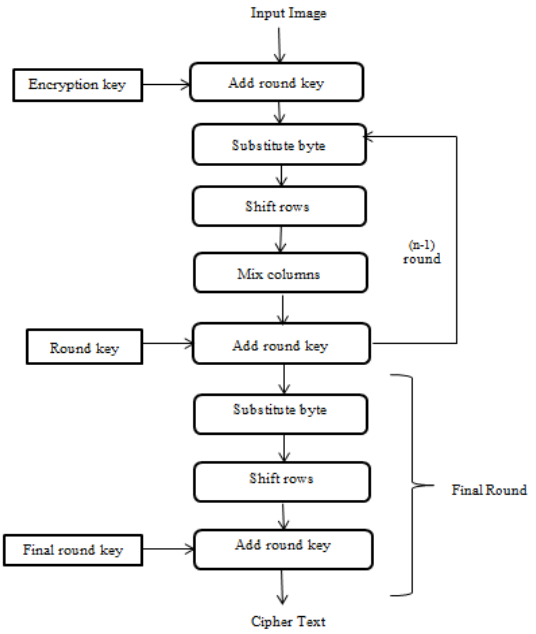

Fig.3.4.1. Flow chart of AES Encryption Algorithm

The execution of the AES-128 encryption and deciphering computation with the help of java writing computer programs is finished. In which the data is an image and the key in a hexadecimal association and the yield is comparable to that of a data picture. For encryption process first, disconnecting picture and making it 4*4 byte state for instance matrix structure. Process the quantity of rounds in light of the key Size and broaden the key using our key timetable. Likewise, there are (n-1) rounds performed which are substitute byte, move lines, mix fragments and incorporate a round key[7][8]. The last round "n" does not include mix portion in the accentuation. Figure 3.4.1 shows the flood of the estimation.

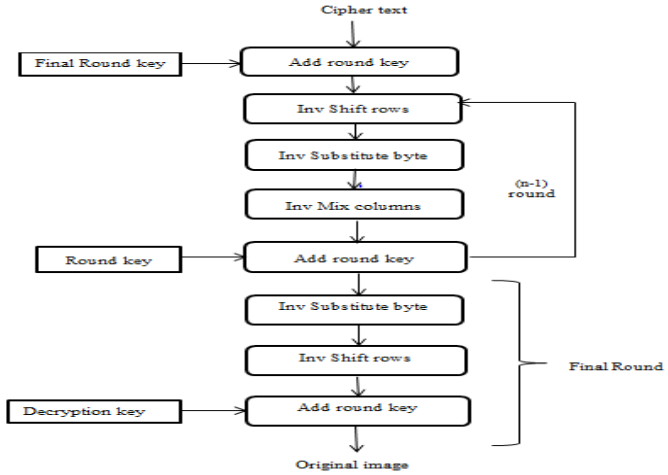

Fig.3.4.2.Flow chart of AES Decryption Algorithm

The AES interpreting process is the pivot method that of the encryption system. The above figure shows the surge of the AES unraveling count. Which involve ciphertext as the information, the key is the proportionate for the deciphering strategy which for encryption. On the off chance that there ought to emerge an event of disentangling the turn around substitute byte, inverse move lines and the regressive mix segments are to be executed. While the incorporate round key proceeds as previously [7].

IV. PROPOSED MODEL

The main purpose of this paper is to secure the medical data using bio-cryptography by taking advantage of fingerprint and cryptographic algorithms. The cryptographic algorithms are used to develop a secure system using fingerprint characteristics. While scanning or any algorithm fails the security questions will come into the module. It will ask some questions which are unknown to other persons and only known to the authorized persons. There are some techniques which are implemented using cryptographic algorithms like RSA, DES, AES, Triple DES, RC4 etc[1]. These are the algorithms used and performed a comparison between the algorithms based on the computing Memory, processing consumption and computing time. By comparing the algorithms they found that the AES algorithm is the most efficient algorithm in mobile platforms[4]. The other techniques are using fuzzy vault and fuzzy commitment algorithms by taking advantage of fingerprint and iris characteristics. Now, this paper is used to provide privacy and security based on the cryptographic algorithms and also the fingerprint module.

V. METHODOLOGY

The main idea of the paper is to secure the records with privacy and authenticity in taking advantage of the fingerprint module and cryptography algorithms. We secure the records as shown in Fig 3.4.1. Initially, the user will be login with his/her login id, password and then open the record using his/her fingerprint which is encrypted and stored in the database. and the record will be opened with high security as shown in Fig 3.4.2. As the fingerprint stored in the database while it was opening the record, it will first check the patient ID with database ID. If the patient ID matches with databaseID it will decrypt the fingerprint and checks whether the fingerprint matches with the database fingerprint and open the record only if it is matched with the database fingerprint.

If the patient is newly registered the patient will go to the options register and fill the application form then scan the finger with the help of fingerprint scanner and add the fingerprints of the patient, administrator, and guardian. The fingerprints of the patient, guardian, and administrator will be secured using encryption algorithm and then stored in the database.

VI. RESULTS

The result obtained by this project is to open the medical records with security and privacy using cryptography algorithms and fingerprint module. While comparing with other algorithms by using AES algorithm we can have high security for the records to prevent unauthorized access. It is highly secured because the record opens only if the patient fingerprint matches with the Database fingerprint. Thus we can make sure that we can protect the patient's data by using this technique.

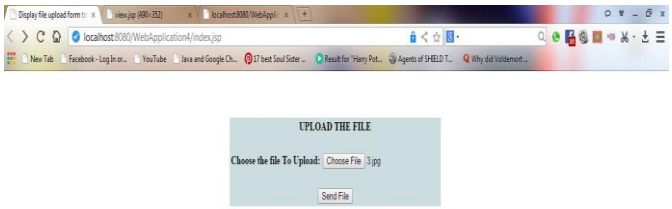

Fig.6.1.Uploading a fingerprint the database

The finger print will be uploaded to the database using NetBeansIDE.firstly,the fingerprint will be encrypted and stored in the database.The patient will be login using his/her patient id and when the id matches the encrypted fingerprint will be decrypted and checks whether the original fingerprint matches with decrpted fingerprint.If the fingerprint matches with database fingerprint then the record will be opened.

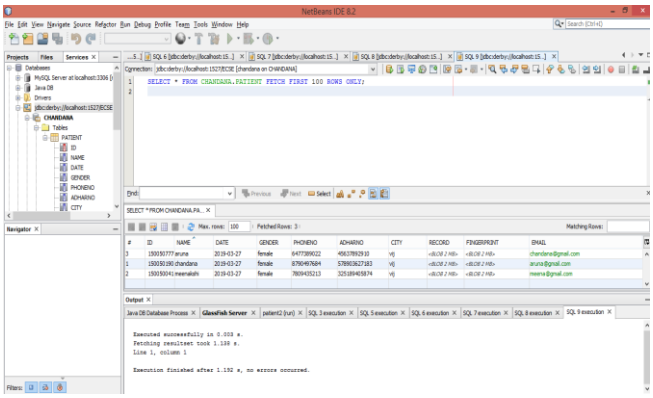

Fig 6.2.successful storing of fingerprint to the database

Fig.6.3.Opening the record using fingerprint

The fingerprint will be encrpted as well as decrypted using built-in functions.Then the fingerprints checks with the database fingerprint and opens the record.

VII. CONCLUSION

This project is aimed to secure health records using bio cryptography. Encryption and Decryption process are done while sending and receiving the data. The code is developed for this process by using NetBeans IDE. And database connection is also given to the patient's data. To secure the records .Thus we can ensure that we can protect the hospital data by using this technique .We can secure the medical records using various algorithms.

REFERENCES

1. Electronic Medical Records in Mobile Platforms , Indian Journal of Science and Technology, Vol 8(21), DOI: 10.17485/ijst/2015/v8i21/60739, September 2015 Study of Cryptographic Algorithms to Protect Jorge E. Camargo et al Faculty for Computing and Systems Engineering, Antonio Narino University, Bogota, Colombia;JorgeCamargo@uan.edu.co,diesierra@uan.edu.co,yeitorres@uan.edu.co
2. Nayer Jamshed1, Fouzia F.Ozair , et al Department of Health Services, Jawahar Lal Nehru University,Department of Emergency Medicine, All India Institute of Medical Sciences,2Department of Forensic Medicine , Hamdard Institute of Medical Sciences and Research, New Delhi, India. Ethical issues in electronic health records: A general overview Perspectives in Clinical Research | April-June 2015 | Vol 6 | Issue 2
3. Ensuring patients' privacy in a cryptographic-based electronic health records using bio-cryptography by Adebayo Omotosh Int. J. Electronic Healthcare, Vol. x, No. x, xxxx 1 Copyright © 200x Inderscience Enterprises Ltd .
4. Appari, A. and Johnson, M.E. (2010) 'Information security and privacy in healthcare: current state of research', International Journal of Internet and Enterprise Management, Vol. 6, No. 4,pp.279–31
5. Brandt M et al Health informatics standards and information transfer: exploring the HIM role (AHIMA Practice Brief). Journal of AHIMA. 2001; 72(1):68.
6. An image encryption and decryption using AES algorithm, IJERT, Volume 7, Issue 2, February-2016 ISSN 2229-5518.
7. Image encryption and decryption using AES algorithm (IJECET), ISSN 0976 – 6464(Print), ISSN 0976 – 6472(Online), Volume 6, Issue 1, January (2015), pp. 23-29 © IAEME
8. Distributed Attribute Based Encryption for Patient Health Record Security under Clouds, Abraham, S. E. (2013).
9. Manjula N Harihar et al(2012, June). "Image Encryption and Decryption using AES",IJEAT volume-1, issue-5
10. Kundankumar RameshwarSaraf, Vishal PrakashJagtap, Amit Kumar Mishra, (2014, May-June)."Text and Image Encryption Decryption Using Advance Encryption Standard", International Journal of Emerging Trends and Technology in computer science(IJETTCS) volume-3, issue-3