ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

A SECURED BIOMETRIC CLOUD BASED APPROACH FOR HEALTH CARE SYSTEM

Dr.J.B.Shajilin Loret[1],I.Meenamarakatham[2],S.Sherin Fathima[3],R.Paulin Jeyapriya[4]
[1] Associate Professor, Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, Tamilnadu.
[2,3,4] UG Students, Department of Information Technology, Francis Xavier Engineering College, Tirunelveli, Tamilnadu.

I.Abstract:

Within the literature, we have witnessed in the healthcare sector, the growing demand for and adoption of software development in the cloud environment to cope with and fulfill current and future demands in healthcare services. In this paper, we propose a flexible, secure, cost-effective, and privacy-preserved cloud-based framework for the healthcare environment. We propose a secure and efficient framework for the government EHR system, in which fine-grained access control can be afforded based on multi-authority ciphertext-policy attribute-based encryption (CP-ABE), together with a hierarchical structure, to enforce access control policies. The proposed framework will allow decision-makers to develop the healthcare sector and to benefit from the existing e-government cloud computing platform ``Yasser," which is responsible for delivering shared services through a highly efficient, reliable, and safe environment. This framework aims to provide health services and facilities from the government to citizens (G2C). Furthermore, multifactor applicant authentication has been identified and proofed in cooperation with two trusted authorities. The security analysis and comparisons with the related frameworks have been conducted.

Keywords: Biometric, Hospital management, Cloud

II.Introduction:

Hospital management system is a computer system that helps manage the information related to health care. They also contain data related to all departments of healthcare. In the entire government healthcare systems, Patient's health record are stored in files and being accessed manually, which has the security threats. To overcome this we have introduced the secured biometric cloud based system. The Main objective of this **Secure Cloud-based Hospital Management System** is to develop software which is user friendly simple, fast, and cost – effective. It deals with the collection of patient's information like add new patient, update patient, search patient history, view patient diagnosis, etc. Traditionally, it was done manually.

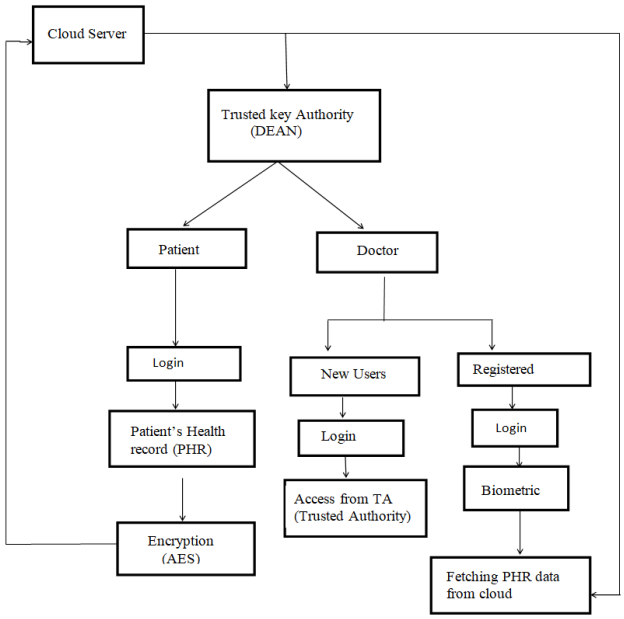
ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

The main function of the system is register and store patient details and doctor details and retrieve these details as and when required, and also to manipulate these details. The doctors can login using a unique username and password. If the doctor is a new user he/she can be authorised by the trusted Authority. The patient's data can be stored in the cloud database by **Advanced encryption standard (AES) encryption algorithm**. The patient diagnosis record can be retrieved only by the biometric information of the doctors. The data are well protected for personal use and makes the data processing very fast.

Government of India has still aimed at providing medical facilities by establishing hospital. The basic working of various hospitals in India is still on paper as compared to hospitals in European countries where computers have been put in to assist the hospital personals their work. The concept of automation of the administration and management of hospital is now being implemented in India also, with large hospitals like APPOLO and AIIMS in Delhi, ESCORTS in Chennai, having automated their existing system.

III.Methodology:



IV.Modules:

1. Trusted Key Authority
2. Patient
3. Doctor

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

1.Patient:

Every patient will have their own unique Identification number (ID) issued by the Trusted Authority. The Patient History Records (PHR) are encrypted by using AES algorithm and stored in cloud server. PHR is fully secured and protected by defining an (attribute based) access policy that can be used for encrypting the data before it is distributed.

2.Doctor:

New Doctor:

If a new Doctor need a access to retrieve a patients record in an emergency case , he/she must needed to get authorized by Trusted Key Authority and then he/she will provided with unique ID and then he/she can able to read a patient detail. During registration process, the doctors are grouped based upon their respective Post Graduate specialization field.

Already Registered Doctor:

When the already registered doctor needs to access the particular patient's data, in addition to the login with their respective unique user ID they have to use the biometric information to fetch the patient's record. Once the fingerprint matches, doctor can access the Patient History records (PHR) for the treatment purposes. In case of emergency cases, where the doctor isn't available, registered doctors to whom the specify doctor give access of the particular specialization department can access the PHR to provide immediate treatment to the patients under critical stage.

4.Trusted Key Authority:

Dean will have all the authorization powers like providing access to all the concerned doctors. Dean has the ability to give access and remove access for any respective doctors. He will have the authorization to access the databases. He can fetch and retrieve the patient’s data at any point of time. Simply Dean is known as trusted authority. He has entire access over the hospital management and healthcare systems.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

V. Result and Analysis:

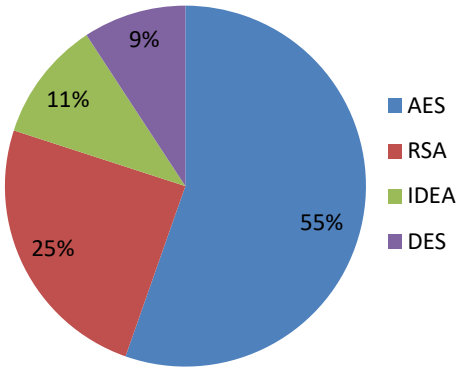


Figure1 Comparison chart

Figure 1 illustrates the comparison of various encryption algorithms based on the overall efficiency. The chart clearly explains that AES algorithm serves the best when comparing to others. AES algorithm provides more security than others and also the speed of execution will be faster. DES is comparatively less efficiency when compared to all other encryption algorithms and the second algorithm with least efficiency is International data encryption algorithm(IDEA).Rivest-Shamir-Adleman is an encryption algorithm with 25 percent algorithm. On comparing to all the other algorithms, AES is found to be more efficient and provides high level data security with encryption and decryption process.

VI. Conclusion:

In this paper, we proposed a secure cloud-based EHR framework that guarantees the security and privacy of medical data stored in the cloud, relying on hierarchical multi-authority CP-ABE to enforce access control policies. The proposed framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients, and practitioners. In the framework, the attribute domain authority manages a different attribute domain and operates independently. In addition, no computational overhead is completed by the government authority, and multifactor applicant authentication have been identified and proofed. The proposed scheme can be adopted by any government that has a cloud computing infrastructure and provides treatment services to the majority of

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 4, April 2021

citizen patients. Future work includes implementing and evaluating the proposed scheme in a real-world environment.

REFERENCE PAPER

[1] M. Masrom and A. Rahimli, ``A review of cloud computing technology solution for healthcare system," *Res. J. Appl. Sci., Eng. Technol.*, vol. 8, no. 20, pp. 2150_2155, 2014.

[2] A. Hucíková and A. Babic, ``Cloud Computing in Healthcare: A Space of Opportunities and Challenges," *Transforming Healthcare Internet Things*, vol. 221, p. 122, 2016.

[3] H. Yang and M. Tate, ``A descriptive literature review and classification of cloud computing research," *CAIS*, vol. 31, Apr. 2012, Art. no. 2.

[4] N. Khan and A. Al-Yasiri, ``Identifying cloud security threats to strengthen cloud computing adoption framework," *Procedia Comput. Sci.*, vol. 94, pp. 485_490, Jan. 2016.

[5] K. Hamlen, M. Kantarcioglu, L. Khan, and B. Thuraisingham, ``Security issues for cloud computing," *Optimizing Inf.Security Advancing Privacy Assurance: New Technologies: New technol.*, vol. 150, 2012).

[6] Manvjeet Kaur, Mukhwinder Singh, AkshayGirdhar, and Parvinder S. Sandhu, *"Fingerprint Verification System using Minutiae Extraction Technique"*.

[7] M. E. Smid and D. K. Branstad, *"Data Encryption Standard: past and future,"* Proceedings of the IEEE, vol. 76, no. 5, pp. 550–559, 1988.

[8] Ako Muhamad Abdullah-*"Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data"*. Article · June 2017.