TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 1781 - 1786

Security and Privacy Preserving for Patient's E-Health Care Applications

A. Sonya[1], G. Kavitha[2], C. Dinesh Kumar[3]
[1,2,3]*B.S.Abdur Rahman Crescent Institute of Science and Technology, India, Chennai.*
Sonya.yasmin152@gmail.com

Article Info
Volume 82
Page Number: 1781 - 1786
Publication Issue:
January-February 2020

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *07 January 2020*

Abstract

Electronic Health (e-Health) acts as a major part in preserving the patient's physical data. In the developing countries like India, the patient's data are stored documental and sharing of patient's physical data leads to lack of privacy and security. In this work, the Attribute Based Encryption (ABE) scheme is adopted to encrypt the patient personal and physiological information. Also, the Clinical Document Architecture (CDA) is utilized for the integration of multiple CDA documents per patient into a single CDA document in cloud computing environment. By analyzing the security and performance of our proposed scheme, leads to various advantages such as high flexibility, availability, integrity, data security etc. This work appears to be high significance since security and privacy are two main factors to be considered for e-Health applications.

Keywords : *Clinical Data Architecture; Cloud; e-Health; Personal Health Record; Privacy; Security.*

I. INTRODUCTION

In recent years, the aging population, dietary habits, hereditary factor, sedentary lifestyles of corporate employee's etc results in increasing prevalence rate of diseases such as mental stress, heart disease and diabetics [1]. The Department of Health and Human Services in US has reported that two million Americans people suffered with mental illness and didn't seek treatment due to privacy concerns, [2],[3]. Most of the chronic diseases could be cured if automated and early detection/diagnostic systems are available.

Electronic Health Services (EHS) gains more importance which is increasingly utilized by doctor personnel's, policy makers, patients etc. Also, the EHS leads to increase in privacy, security and integrity of healthcare information or data. Recent health-care systems/e-health systems, integrated with medical sensors or Internet of Things (IoT) devices, wireless connectivity/ communication device, computing device, cloud server etc. gives virtual consultations or treatments to patients remotely which is provided by doctors from hospitals/clinics.

Several researchers have adopted e-health systems for treatment of various diseases [4-8].Zhang et al. (2018) [4] have developed a Cloud-based Electrocardiogram system for the diagnosis of Acute Myocardial Infraction (AMI) patients. Also, the authors have concluded that the ECG's of the AMI patients can be monitored directly using existing smart phone with fewer Doors to Balloon time. An e-Health system has applications such as multimedia conferencing, access to Electronic Health Records (EHR), medical image/video streaming, patient vital signs transmission etc. It is essential to achieve high security and privacy in e-Health systems to provide high quality patient care. Various researchers have introduced secure algorithms to ensure high level of privacy and security [9-12].Winnie et al. (2018) [12] have designed a system using DS 18B20 temperature sensor to collect human temperature data. Further, the authors have encrypted the collected data in fog node using Advance Encryption Standard (AES) algorithm. Also, the authors have concluded that the

January - February 2020
ISSN: 0193 - 4120 Page No. 1781 - 1786

proposed system has high security than the conventional Internet of Things (IoT) cloud architecture. Azeez and Van der Vyver (2018) [9] have discussed on major lack of security issues on this cloud computing environment for e-health applications. Sudheep and Joseph (2019) [10] have discussed various methods to secure medical data in cloud environment. Further, the authors have utilized decoy technique to store and access medical healthcare data. Also, the authors have concluded that the fog computing is highly efficient. Srilakshmi et al. (2019) [11] have designed an intelligent patient's clinical care system in the application layer of Software Defined Networking (SDN). Further, the authors have concluded that the proposed system can protect the confidential information of patient health reports.

The proposed work is to develop a system to secure and preserve Patient Clinical Records (PCR).

II. METHODOLOGY

Figure 1 shows the framework for security and privacy preserving for medical data.

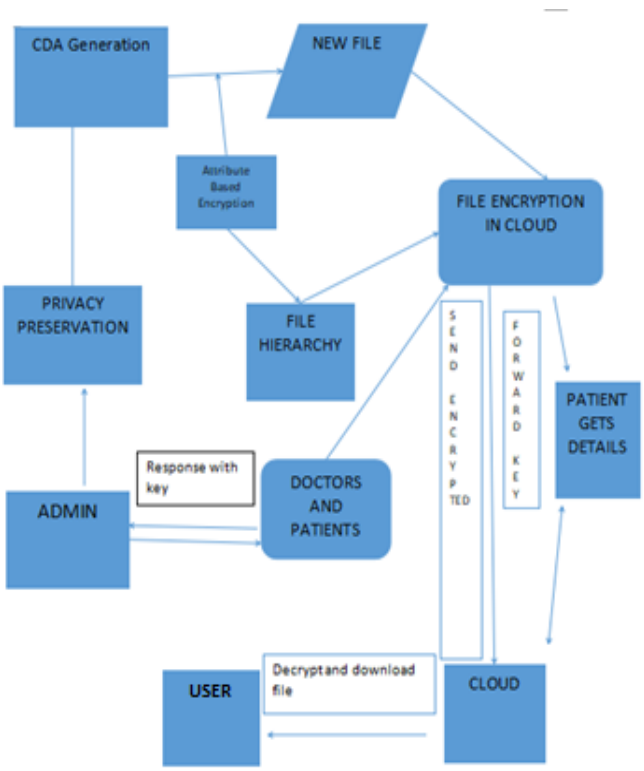

Figure1: Privacy preserving for medical data

The proposed work consists of various sub process such as analysis and authority, user information/data, file hierarchy, third-party auditor, clinical document architecture, attribute-based encryption and cloud storage.

a) Identity and authority

Approved administrators and unapproved administrators can't effectively separate the identifies of the client from one another. Just the administrators straightforwardly approved by the clients can get to the client's close to home wellbeing data and touchy data and can verify their identities at the same time. The various administrators in an approved by the client can't verify the client's identities however recuperate the person clinical data.

b) User information/data

In this work, the Patient Health Record (PHR) in cloud computing environment can be shared securely by dividing it into two parts namely patient's personal information D1 which contains details such as user's login name, identity number, personal mobile number, residential address, etc. and the medical report data D2 which contains patient's physiological data like as clinical verification results, previous clinical treatment and overall patient's clinical history reports. The information D1 and D2 can be encrypted by adopting CP-ABE scheme with various access methods based on the actual need.

c) File Hierarchy

In the proposed work, the many-layered access structures are incorporated into a one-time access structure and the encryption of various file Hierarchy leveled records are finished utilizing incorporate access structure leads to advantages such as less ciphertext storage, less computation time, less cost of encryption etc. Also, the File Hierarchy Ciphertext policy Attribute-based encryptionscheme (FH-CP-ABE) can successfully resists chosen plaintext attacks.

January - February 2020
ISSN: 0193 - 4120 Page No. 1781 - 1786

A physician requires both the patient's personal profile as well as his previous medical record/historyfor the effective diagnosis, whereas the medical researcher requires clinical verification results for academic purpose. If the patient sets the access structure of D1 as: M1 {("Cardiology" AND "Researcher") AND "Attending Physician"} similarly, D2 is termed as: M2 {"Cardiology" AND "Researcher"} the patients clinical data need to be encrypted twice if D1 and D2 are encrypted with access structures M1 and M2, respectively. The two structures could be corporate into one structure M. Due to the above discussed process, the processing difficulty of encryption and capacity overhead of cipher text can be reduced. [13].

d) Third-Party Auditor

In this process, the third-party Auditor (TPA) can access or view all the files uploaded by patient/User without any password key. Further, the third-party Auditor has rights to encrypt the user's data and store it on cloud. Also, the auditor can maintain and supervise the clinical data which is uploaded by various other users. TPA can scramble information and send it to Cloud specialist organization (CSP) for capacity and the examiner can see encoded information of each client.

e) Clinical Document Architecture

In recently, doctors have to distribute the patient information from one hospital to another hospital by documental reports. Usually, Doctor's/Hospitals do not keep any database. Presently, the patient needs to carry all their medical treatment documents and booklets. Moreover, it won't be in an order. To overcome all the above discussed drawbacks the Clinical Document Architecture (CDA) is utilized. The CDA document generation and integration service based on cloud computing, through which hospitals are enabled to conveniently generate CDA documents without having to purchase proprietary software.Further, secure and preserve Patient Clinical Records is done using Slicing algorithm. The Clinical Document Architecture (CDA) is utilized in this work to integrate multiple CDA files patients into a unique single CDA file. Also, the discussed process saves hospital money rather purchasing proprietary software for CDA file generation and integration service based on cloud computing. The single unique CDA file generation helps the physicians and patients to search and access the clinical data in temporal or historical order which results in easy understanding of patient conditions from the previous verification tests and medicines been taken and symptoms in a single file.

f) Attribute-based encryption

Attribute-based encryption (ABE) reckons the concept of public-key cryptography [14], [15]. A text or information is encrypted using receiver's public key for a specific receiver in conventional public-key cryptography. Further, the Identity-based cryptography/encryption (IBE) uses arbitrary string as a public-key.

g) Cloud Storage

In general, the personal information and medical records of the patients can be stored on the cloud storage for e-health applications. It is essential to protect the patients personal and health information. For this security purpose, all the information's are encrypted using ABE algorithm. In general, there are N number of public online cloud storages are available in which the files can be shared and collaborated.In this work, the public cloud named CloudMe cloud storage is utilized as a cloud storage. The utilized cloud has 2 gigabytes (GB) of storage for free of cost and the storage can be extended for various payment plans. By using the CloudMe cloud storage service the personal and health information data's are stored in the remote cloud servers and the files are shared in a synchronized format. CloudMeis capable of storing any kind of file typessuch as medical images, Microsoft document files, videos etc.

January - February 2020
ISSN: 0193 - 4120 Page No. 1781 - 1786

III. DISCUSSIONS

Figure 2 shows the administrator's home page in which the menu's such as reception, doctor personnel's availability, patient registration, doctor registration, patient details and session logout menus are incorporated. Once administrator/receptionist has signed in, the above-mentioned menus can be accessed.

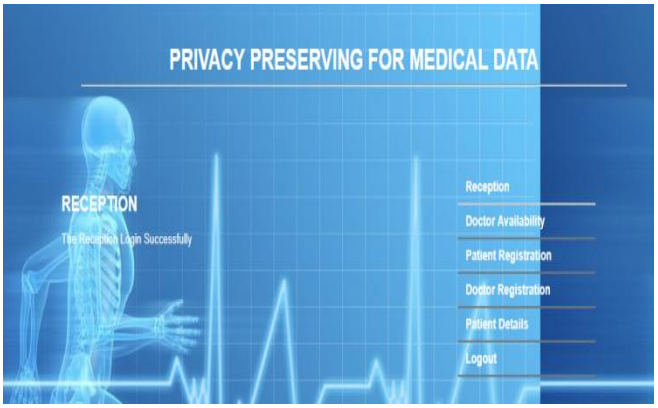

Figure 2: Administrator's home page

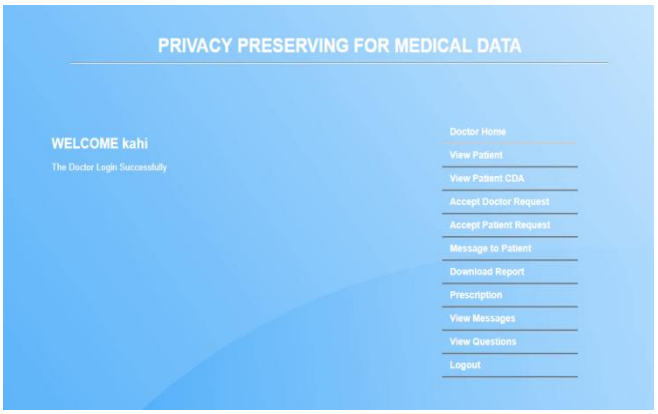

Figure3: Doctor Personnel's home page

Figure 3 shows the home page of doctor personnel in which the menus such as view patient, view patient CDA, accept doctor request, accept patient request, message to patient, report download, prescription, view messages, view questions and doctor personnel logout menus are incorporated.

Figure4: User Login Page

Figure 4 shows the User login page by which user can sign up to access/view their own medical record.The proposed work has several advantages such as flexibility, availability, integrity, data privacy and security etc.

a) Flexibility

The users namely patients and doctor personnel can access/view data which results in high flexibility. Also, the proposed system can replace conventional paper bills and physical file records. One can access/view the medical data without any difficulty since the webpage is created in such a way.

b) Availability

The Patient Health Report can be accessed anywhere and anytime with a developed e-health system. Since the data is stored on cloud, results in no data loss due to natural calamities.

c) Integrity, Data privacy and security

The personal information each and every patient is open to authorized users. Further, the medical data is encrypted to avoid any alterations. Also, the patient information and physiological conditions are divided and the privacy of the information is preserved since the slicing algorithm is utilized.

IV. CONCLUSION

Nowadays, e-heath gains high prominence due to

January - February 2020
ISSN: 0193 - 4120 Page No. 1781 - 1786

various advantages such as data availability, decentralized access etc. Also, it is essential to secure both patients personal and health related information. In this work, the Attribute Based Encryption (ABE) scheme was adopted to encrypt the patient personal and health information. Further, the CDA was used for the integration of multiple CDA documents per patient into a single CDA file in cloud. Also, it is clearly observed that the privacy, security etc. of the proposed scheme has high flexibility, availability, integrity, data security etc. The proposed work can also be extended to view human vital signs, physiological states etc. with high security and privacy in near future.

REFERENCES

[1] Yau, J.W., Rogers, S.L., Kawasaki, R., Lamoureux, E.L., Kowalski, J.W., Bek, T., Chen, S.J., Dekker, J.M., Fletcher, A., Grauslund, J. and Haffner, S., 2012. Global prevalence and major risk factors of diabetic retinopathy. Diabetes care, 35(3), pp.556-564.

[2] Yüksel, B., Küpçü, A. and Özkasap, Ö., 2017. Research issues for privacy and security of electronic health services. Future Generation Computer Systems, 68, pp.1-13.

[3] Aghili, S.F., Mala, H., Shojafar, M. and Peris-Lopez, P., 2019. LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Future Generation Computer Systems, 96, pp.410-424.

[4] Zhang, X.S., Leu, F.Y., Yang, C.W. and Lai, L.S., 2018. Healthcare-based on cloud electrocardiogram system: A medical center experience in middle Taiwan. Journal of medical systems, 42(3), p.39.

[5] Yahyaie, M., Tarokh, M.J. and Mahmoodyar, M.A., 2019. Use of Internet of Things to Provide a New Model for Remote Heart Attack Prediction. Telemedicine and e-Health, 25(6), pp.499-510.

[6] Xia, H., Asif, I. and Zhao, X., 2013. Cloud-ECG for real time ECG monitoring and analysis. Computer methods and programs in biomedicine, 110(3), pp.253-259.

[7] Chung, W.Y. and Fong, E.M., 2014, August. Seamless personal health information system in cloud computing. In 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (pp. 3658-3661). IEEE.

[8] Fraga-Lamas, P., Fernández-Caramés, T., Suárez-Albela, M., Castedo, L. and González-López, M., 2016. A review on internet of things for defense and public safety. Sensors, 16(10), p.1644.

[9] Azeez, N.A. and Van der Vyver, C., 2018. Security and privacy issues in e-health cloud-based system: A comprehensive content analysis. Egyptian Informatics Journal (dec 2018).

[10] Sudheep, K. and Joseph, S., 2019, March. Review on Securing Medical Big Data in Healthcare Cloud. In 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS) (pp. 212-215). IEEE.

[11] Srilakshmi, A., Mohanapriya, P., Harini, D. and Geetha, K., 2019, February. IoT based Smart Health Care System to Prevent Security Attacks in SDN. In 2019 Fifth International Conference on Electrical Energy Systems (ICEES) (pp. 1-7). IEEE.

[12] Winnie, Y., Umamaheswari, E. and Ajay, D.M., 2018, September. Enhancing Data Security in IoT Healthcare Services Using Fog Computing. In 2018 International Conference on Recent Trends in Advance Computing (ICRTAC) (pp. 200-205). IEEE.

[13] Sharon, R.S. and Manoj, R.J., 2017, February. E-health care data sharing into the cloud based on deduplication and file hierarchical encryption. In 2017 International Conference on Information Communication and Embedded Systems (ICICES)(pp. 1-6). IEEE.

[14] Sahai, A. and Waters, B., 2005, May. Fuzzy identity-based encryption. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 457-473). Springer, Berlin, Heidelberg.

[15] Guo, W., Dong, X., Cao, Z. and Shen, J., 2018, September. Efficient Attribute-Based Searchable Encryption on Cloud Storage. In Journal of Physics: Conference Series (Vol. 1087, No. 5, p. 052001). IOP Publishing.

[16] S.Hemalatha and S.Alaudeen Basha,"Enabling for Cost-Effective Privacy Preserving of Intermediate

January - February 2020
ISSN: 0193 - 4120 Page No. 1781 - 1786

Data Sets in Cloud" Journal of Scientific and Research Publications,vol.3 issue.10,oct 2013.

[17] C.Celcia and T.Kavitha, "Privacy Preserving Heuristic Approach for Intermediate Data Sets in Cloud", Journal of Engineering Trends and Technology, vol.9,no.5,march 2014.

[18] A.Sonya, Dr. G.Kavitha, Efficient approaches for storing retrieval and replication of data using cloud system. International Journal of Pure and Applied Mathematics Volume 117 No. 20 2017, 1011-1020 ISSN: 1311-8080 ISSN: 1314-3395 Nov 17.

[19] A.Sonya Clustering of Crime Information by Using Mobile Application, International Journal of Engineering Research & Management Technology September-2018 ISSN: 2348-4039 Volume 5, Issue-5

[20] Kan Yang and Xiaohua Jia," An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing" in the IEEE Transactions on Parallel and Distributed System, Vol. 24, No. 9, September -2013.