ENHANCING THE SECURITY OF CLOUD STORAGE FOR MEDICAL DATA RETRIEVAL USING DOUBLE ENCRYPTION WITH DATA ANONYMIZATION

P. Harish, S.Vigneshwari, K.B.S. Ravi Teja

School of Computing, Sathyabama University, Tamilnadu, India
Email: harishben1@gmail.com, vikiraju@gmail.com, teja.ravi145@gmail.com

ABSTRACT

Now-a-days the major issue that was seen in hospital management is providing security to the patient's related data. Such data's are so sensitive, exploiting that type of data may result in leakage of patient's information. They are some previous systems which provide security to the patient's data, but the algorithms that have been issued are timing enabled proxy re-encryption algorithms, which issues keys and to use them within in the time limit, so these causes in some difficulty to user in order to access his data whenever he wants. In order to overcome this type of encryption processes we propose a double encryption with anonymization technique and implementation of multiple health records in a cloud server. Whenever the user wants to retrieve the information from the cloud server, user gets a one-time password to his registered email id.

Keywords: Security, Cloud, Anonymization, PHR, AES.

I. INTRODUCTION

An Electronic Health Record (EHR) is an electronic form of a patient's therapeutic history maintained in the server which is very useful for the users to access the data through their respective device from any- where they want. Security is a noteworthy concern with regards to electronic wellbeing records. Utilizing EHR programming can possibly put your association at hazard on the off chance that you don't take after security conventions to a demanding degree. While paper records additionally make it simple to abuse a patient's security, the comfort and promptness of electronic records make it less demanding to damage protection at an extraordinary leve l. Here we are using proxy re-encryption method (PRE). Proxy re-encryption plans are cryptosystems which permit outsiders (intermediaries) to adjust a cipher text which hosts been encoded for one get- together, with the goal that it might be unscrambled by another.

II. REVIEW OF RELATED WORK

An Electronic Health Record (EHR) is an electronic form of a patient's therapeutic history maintained in the server which is very useful for the users to access the data through their respective device from any-where they want. Security is a noteworthy concern with regards to electronic wellbeing records. Utilizing EHR programming can possibly put your association at hazard on the off chance that you don't take after security conventions to a demanding degree. While paper records additionally make it simple to abuse a patient's security, the comfort and promptness of electronic records make it less demanding to damage protection at an extraordinary level. Here we are using proxy re-encryption method (PRE). Proxy re-encryption plans are cryptosystems which permit outsiders (intermediaries) to adjust a cipher text which hosts been encoded for one get-together, with the goal that it might be unscrambled by another. Leventhal, et al., [1] discussed about We examine the issue of seeking on information that is scrambled utilizing an open key framework.

PEKS schemes can permit a client to look encoded information privately, a large portion of them neglected to confirm the sought result and the framework did not indicate the clients who can make a demand for scrambled information records put away on the cloud server [2].

PEKS secure against watchword specu- lating assault is just secure under the irregular prophet display, which does not mirror its security in this present reality. Moreover, there is no entire definition that catches secure channel free PEKS plans that are secure against picked watchword assault, picked cipher text assault, and against catchphrase speculating assaults, even though these ideas appear to be the most pragmatic use of PEKS primitives [3].

Boneh, et al., [4] the plan that looking over the encoded information, which is additionally named conjunctive catchphrase searchable conspire, empowers one to look the scrambled information by utilizing conjunctive catchphrases. e. Be that as it may, there are still spaces for both sorts of the plans to make strides both the execution and the security.

Tang, et al., [5] the issue of conjunctive with subset catchphrases seek work, examine the downsides about the existed plans, and afterward give out a more proficient development of Public Key Encryption with Conjunctive-Subset Keywords Search (PECSK) conspire. A correlation with different plans about effectiveness will be introduced. We likewise list the security prerequisites of our plan, and then give out the security investigation.

Liu, et al., [6] security display has not been founded on social databases, for example, Oracle and MS-Access, consequently it is difficult to apply them practically speaking. In addition, they have not considered a critical security thought for client's trapdoor inquiries. In this paper, we first formally characterize a security show for conjunctive watchword seeks plans including trapdoor security considering a down to earth social database.

Fang, et al., [7] The Public Key Encryption with Conjunctive Keyword Search (PECK) conspire empowers one to look a report incorporated various scrambled catchphrases without trading off any unique information data. The current PECK conspires for the most part rely on upon pairings and verified channel to accomplish searchable encryption.

Hwang, et al., [8] searchable intermediary re-encryption plot (Re-PEKS), characterize the primary known searchable intermediary re-encryption plot with an assigned

analyzer (RedPEKS), and afterward give solid developments of both Re-PEKS and Re-dPEKS plans that are secure in the arbitrary prophet show, alongside the confirmations.

Bharathi and Kumar [9] cryptographic primitive called contingent intermediary re-encryption with catchphrase seeks (CPRES), which joins C-PRE and PEKS. We take note of that there are nuances in joining these two thoughts to accomplish a protected plan, and thus, the mix is not inconsequential.

Bharathi and Kumari [10] cryptographic primitive called public key re-encryption with watchword seek (PRES). The principle curiosity all the while understands the usefulness of intermediary re-encryption and watchword seeks in one primitive, it was a theoretical assumption of the encryption algorithm which is not yet been implemented.

Data hiding and encryption mechanisms were discussed [11, 12]. Classification, clustering and similarity comparison were discussed [13]. Data mining and hazy semantics approach with enhanced security has been discussed in [14, 15].

III. ALGORITHM

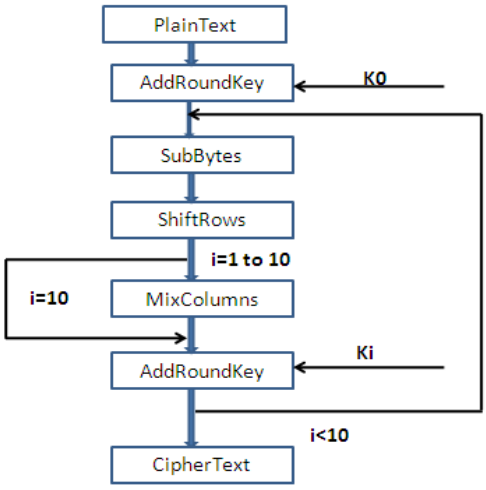

Fig 1.0. AES Algorithm flow

AES Encryption algorithm is used for providing security to the user's health records. Where all the information stored in cloud has been in the encrypted format. This algorithm is used for storing records securely explains this in Fig 1.0.

IV. PROPOSED SYSTEM

Proposed system was applied timing enable proxy re-encryption searchable encryption model to electronic health records (EHR) to formally proved secure against chosen-keyword chosen-time attack. Furthermore, off-line keyword guessing attacks can be resisted too. Data owner outsource their encrypted data to EHR storage provider. Proxy server encapsulates the data into re-encryption cipher text.

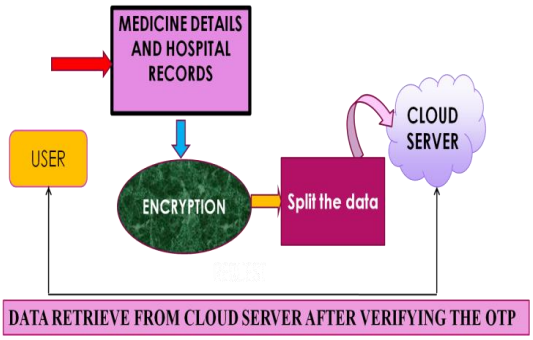

Fig 2.0 Module Description

An Architecture Diagram shows how a user can store the details in a form of security. First user gives their medical details it was stored on the server in an encrypted format. The module classification is given in Fig 2.0. Finally, anyone wants to view the information means they get from the OTP verification process [16].

V. MODULES

A. Cloud server deployment

In this module, main cloud server is deployed. Within this all access are maintained and monitored. Main server contains all details about service provide and user's information. If any new request comes from the user then sever will collect all request and process that request. Based on the request it will redirect it to that service providers. In this cloud server, all hospital's information is maintained.

B. Hospital Deployment

In this module hospital server is deployed known as secondary server which contains information about their respective hospitals and their user details.

C. User Registration

The client detail like username, secret word, client individual points of interest and cloud server with administration supplier subtle elements are saved into the Server. After registration client can login and can access the cloud server information

D. Mongo Lab– User Data Separation

Mongo DB is an open-source record database and driving No SQL database. Mongo DB is used to make and convey a profoundly adaptable and execution situated database. Mongo DB is a cross-stage record situated database. In this module store the data about client profile like client name, password, Email id, phone number and medicinal reports.

E. Double encryption & data Anonymization

In this module, we can plan and usage of twofold encryption for patient individual data likes name, infection and so forth. Information anonymization is a kind of data purification whose expectation is security assurance. It is the procedure of either scrambling or evacuating by and by identifiable data from data sets, so that the general population whom the data describe stays unknown.

F. Dynamic Data Transfer

Client needs to therapeutic points of interest means, simply demand to cloud server. At the time produce one OTP and sent to your mail id for check prepare. At long last confirm the OTP short time later just information is exchanged or recovered from cloud server.

VI. RESULTS

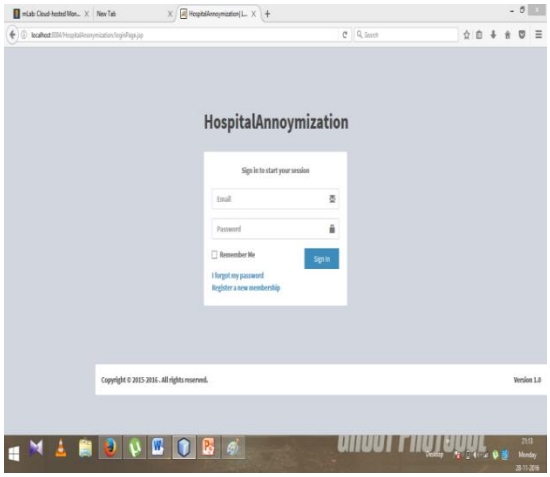

Fig 3.0 Registration Form

Fig 3.0 describes about the prototype of the user registration form in which user can sign up for new Account or user can log in with his existing account.

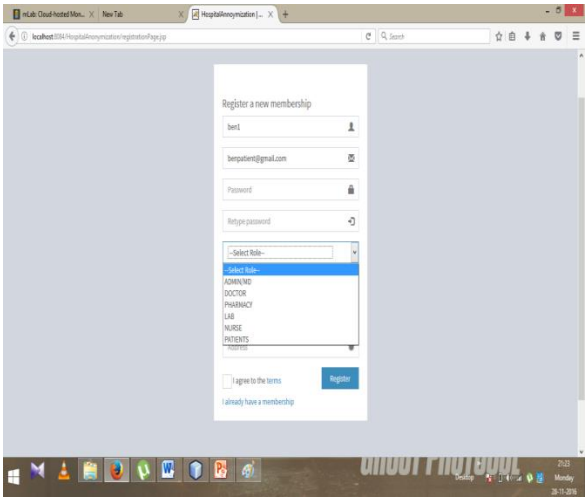

Fig 3.1 User Sign up Form

Fig 3.1 describes about the respective users like patient, doctor, Lab assistant etc, can sign up with their respective details

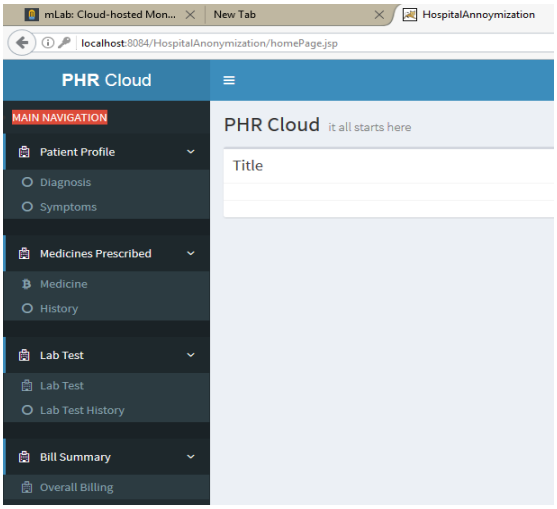

Fig 3.2 Dash Board of Patient Profile

Fig 3.2 represents Dashboard of the Patient Profile

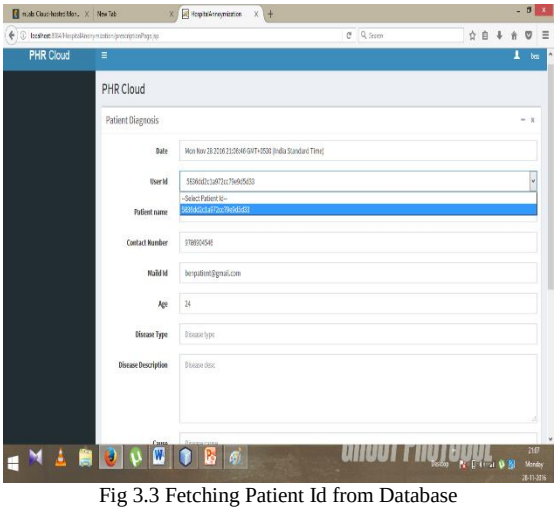

Fig 3.3 Fetching Patient Id from Database

This Figure explains about the fetching the Patient data from the data base using their Patient Id's.

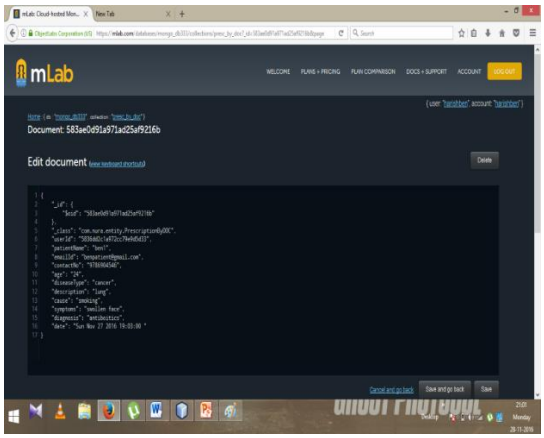

Fig 3.4 Data Storage in MongoDb

Fig 3.4 describes about the storage of patient health data and his personal information and about the users who are all registering in the website in a structural format.

TABLE 1: USER DETAILS

User Category	Users with Full Access	Users with Partial Access	Denial of Access
Doctor	10	N.A	N.A
Patient	50	N.A	N.A
Lab	N.A	50	N.A
Nurse	N.A	20	N.A
Pharmacy	N.A	1	N.A

Table 1 describes the user details. The various categories of users are Doctor, Patient, Lab Technician, Nurse, Pharmacist out of 130 users. Since the users are hospital staffs, there will be no denial of access. The access will be denied only for third party people and outsiders.

VII. CONCLUSION

Finally, we done twofold encryption with oddity method is actualized for the put away in cloud servers. In this work, understanding information can be exchan-ged to various health facilities with element exchange. Contrasted and other established encryption conspires; the productivity investigation demonstrates that our proposed plan can accomplish high calculation and capacity proficiency other than its higher security.

ACKNOWLEDGMENT

I would like to thank Sathyabama University for giving me opportunity to work in the DST-FIST sponsored Cloud Computing Lab (order Saction No. SR /FST/ETI-364/2014) School of Computing, Sathyabama University.

REFERENCES

[1] J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney, Designing a system for patients controlling providers' access to their electronic health records: Organizational and technical challenges. J. General Internal Med. 30(1): 17–24 (2015).

[2] Microsoft. Microsoft HealthVault. [Online]. Available: http://www. healthvault.com, accessed May 1, (2016).

[3] Google Inc. Google Health. [Online]. Available: https:// www. Google.com/health, accessed Jan. 1, (2016).

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, Proc. EUROCRYPT, vol. 3027. Interlaken, Switzerland Pp. 506–522 (2004).

[5] Q. Tang, Public key encryption schemes supporting equality test with authorisation of different granularity. Int. J. Appl. Cryptogr. 2(4): 304–321 (2012).

[6] P. Liu, J. Wang, H. Ma, and H. Nie, Efficient verifiable public key encryption with keyword search based on KP-ABE, Proc. IEEE 9th Int. Conf. Broadband Wireless Computer Commune. Appl. (BWCCA), Pp. 584–589 (2014).

[7] L. Fang, W. Susilo, C. Ge and J. Wang, Public key encryptt-ion with keyword search secure against keyword guessing attacks without random oracle. Inf. Sci. 238: 221 – 241 (2013).

[8] M.-S. Hwang, S.-T. Hsu, and C.-C. Lee, A new public key encryption with conjunctive field keyword search scheme. Inf. Technol. Control 43(3): (2014)

[9] B.Bharathi and Mahesh Kumar, Non-invasive BG scrutinizer system. Global Journal of Pure and Applied Mathematics 12(8): 5123–5125 (2016)

[10] B.Bharathi and Priyanka Kumari, Secure data hiding in image over encrypted domain. ARPN Journal of Engineering and Applied Sciences 11: (2016)

[11] S. Gowri, G. S. Anandha Mala, G. Mathivanan, Classification of Breast Cancer Cells using Novel DPSC Algorithm. Journal of Pure and Applied Microbiology 9 (2): 1395-1400 (2015)

[12] S. Kalpana, S. Vigneshwari, Selecting multiview point similarity from different methods of similarity measure to perform document comparison. Indian Journal of Science and Technology 9(10) 1-6 (2016)

[13] R. Saranya, S. Gowri, S. Monisha, S. Vigneshwari, An ontological approach for originating data services with hazy semantics. Indian Journal of Science and Technology 9(23): 1-6 (2016)

[14] Vijai Chandra Prasad R., Yashwanth Sai M., Niveditha P.R., Sasipraba T., Vigneswari S. and S. Gowri, Low cost automated Facial Recognition system, Second IEEE International Conference on Electrical, Computer and Communication technologies (2017).

[15] S. Vigneshwari and M. Aramudhan, Personalized cross ontological framework for secured document retrieval in the cloud. National Academy Science Letters-India 38 (5): 421–424 (2015).

[16] D. Usha Nandini, A. Ezil Sam Leni, Shadow identification using ant colony optimization. Journal of Theoretical and Applied Information Technology 78(2):195-200 (2015).