Efficient Method of Securing Personal Health Record and Sharing in the Cloud

Karthick .A[1] Manikandan .N[2] Dhineshkumar .V[3] Savitha .K[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]Mahendra Institute of Technology, Namakkal, India

Abstract— Now a day, every process is done based on internet. Each data transaction is held through it with the major support of cloud environment. Cloud is an emerging technology and its application are enhancing day by day due to be various advantages. We can access our data from anywhere at any time. The major issue we faced in cloud environment is security. According to current technology development, health monitoring is held through smart a device which leads to storing of health reports in cloud. As we discussed before security is a major issue therefore our proposed system focuses on securing health reports in cloud environment with more privacy. Initially patient will upload their personal details inorder to create an account and then doctor will handle the report. Whenever patient meets doctor he will generate a random key using Random Key Generator to doctor when doctor is an authorized user he can download the file in encrypted format. In order to open particular file respective file encryption key is needed to decrypt it. Therefore patient health reports will be stored in secure way in cloud by Attribute based encryption (ABE) and without user knowledge even doctor could not access the file.

Keywords: Cloud, ABE, Random Key Generator, Security

I. Introduction

Personal health record is risen as a patient-driven model of wellbeing data trade. These days most of the clients store their wellbeing related data in an outsiders on the Internet. It enables the patient to make and control his/her therapeutic related information which might be set in a solitary spot, for example, data focus. Because of the mind-boggling expense of structure of the touchy individual wellbeing data, particularly when they are put away at an outsider server which individuals may not completely confide in precedent, individual email, information, and individual inclinations are put away on online interface destinations, for example, Google and Yahoo. So in this paper we utilize an encryption called Attribute based Encryption with the goal that individuals will be capable encode their PHR record from wherever they need to. The principle concern is about the security of patients, individual wellbeing information and to discover which client could access the restorative records put away in a cloud server.

In ABE, the properties of clients or information that chooses the entrance arrangements empowers a patient to share their PHR specifically among a lot of clients in the wake of encoding the document based on a lot of qualities. Accordingly, the quantity of qualities included decides the complexities in encryption, age of key and unscrambling.

By utilizing ABE, to address key administration challenges, we partition the clients into two sorts of spaces; they are open and individual area. Besides, the patient will dependably reserve the option to concede, yet additionally disavow get to benefits when the patient feel it is essential. The primary objective of patient-driven protection is struggle with adaptability in PHR framework. The approved clients may either need to get to PHR document for individual use or expert purposes. Usage of norms for human services information, precise patient identification and coordinating of records, and meaning of motivating forces for quickened sending of wellbeing data innovation.

The PHR proprietor them self ought to choose how to scramble their records and to permit which set of clients to get access to each document. A PHR document should just be accessible to the clients who are given the comparing decoding key, while stay secret to the remainder of clients. Moreover, the patient will dependably hold the privilege to allow, yet in addition deny get to benefits when they feel it is fundamental. The objective of patient-driven protection is regularly in strife with adaptability in a PHR framework. The approved clients may either need to get to the PHR for individual use or expert purposes. Outline and usage of acknowledged benchmarks for human services information, precise patient distinguishing proof and record coordinating, and the meaning of motivations for quickened arrangement of wellbeing data innovation. In light of these difficulties, we present in this paper an elective alternative, the Health Record Banking (HRB) framework. Imitating business banking, this methodology utilizes wellbeing record banks to serve the requirement for promptly available and secure information for differing partners.

II. Related works

Sabna A B and Harsha T D, (2015) describes the PHR is a device that you can use to gather, track and offer past and current data about your wellbeing or the strength of somebody in your care. Personal health record (PHR) is considered as a developing patient-driven model of health information trade, where individuals can share their wellbeing data to other individuals. Since there are wide security worries about the wellbeing records and due to high operational cost, clients put away at an outsider server called as Cloud Server. The issues, for example, dangers of protection introduction, versatility in key administration, get to issue, client denial, have remained the most essential difficulties towards accomplishing fine-grained, cryptographically upheld information get to control. In orderto get free offfrom this, in this paper we present quality based encryption (ABE) methods to encode every patient's PHR record with the goal that an unapproved people won't most likely view our PHR document.

JianghuaLiu et.al (2015), presents the sharing of Personal Health Records (PHR) in distributed computing is a promising stage of wellbeing data trade. Be that as it may, the capacity of individual restorative and wellbeing data is typically re-appropriated to some outsiders which may result in the presentation of patients' protection to unapproved people or associations. So as to address this security proviso, we propose a promising arrangement. We propose another methodology for fine-grained get to control and verify sharing of signcrypted (sign-then-encode) information. We call our new crude Ciphertext-Policy Attribute-Based Sign cryption (CP-ABSC) which fulfills the prerequisites of distributed computing situations for PHR. CP-ABSC consolidates the benefits of advanced mark and encryption to give classification, validness, unforgeability, secrecy and arrangement opposition. The accuracy, security and effectiveness of this plan are likewise demonstrated.

Satheesh.K and Ram kumar.A, (2014), discusses the fundamental concern is aboutdiagnosis data. The patient records ought to be whether the patients could really control the imparting kept up to high protection and security. The security plans are utilized to shield the individual information from free. Quiet information can be gotten to by a wide range of individuals. Every specialist is doled out with access consent for a specific arrangement of properties. The entrance control and protection the board is a perplexing undertaking in the patient wellbeing record the board procedure. Distributed computing is a casual articulation used to depict a wide range of kinds of processing ideas that include an expansive number of PCs that are associated through a continuous correspondence organize. It is an equivalent word for conveyed processing over a system and means the capacity to run a program on many associated PCs in the meantime. Information proprietors refresh the individual information into outsider cloud server farms. The epic patient-driven structure and a suite of information get to systems to control PHRs put away in semi-confided in servers. To accomplish fine-grained and versatile information get to control for PHRs, we influence Attribute Based Encryption (ABE) strategies to scramble every patient's PHR document. Numerous information proprietors can get to similar information esteems. The proposed plan could be reached out to Multi Authority Attribute Based Encryption (MA-ABE) for various expert based access control system.

Rakesh. B and Harsha Vardhan. A (2013), presents PHR, is a wellbeing record where wellbeing information and data identified with the consideration of a patient is kept up by the patient. This stands as opposed to the more generally utilized electronic therapeutic record, which is worked by organizations, (for example, medical clinics) and contains information entered by clinicians or charging information to help protection claims. The goal of a PHR is to give a total and exact rundown of a person's therapeutic history which is available on the web. The wellbeing information on a PHR may incorporate patient-announced result information, lab results, and information from gadgets, for example, remote electronic gauging scales or gathered inactively from a Smartphone. To accomplish fine-grained and adaptable information get to control for PHRs, we influence trait based encryption (ABE) methods to encode every patient's PHR document. In Attribute-Based Encryption the unscrambling of a figure content is conceivable just if the arrangement of qualities of the client key matches the characteristics of the figure content. A pivotal security highlight of Attribute-Based Encryption is intrigue opposition: A foe that holds numerous keys should possibly have the capacity to get to information if somewhere around one individual key gifts get to.

Ming Li et.al (2013) describes PHR is a developing patient-driven model of wellbeing data trade, which is regularly redistributed to be put away at an outsider, for example, cloud suppliers. Be that as it may, there have been wide protection worries as close to home wellbeing data could be presented to those outsider servers and to unapproved parties. To guarantee the patients' authority over access to their own PHRs, it is a promising strategy to scramble the PHRs before re-appropriating. However, issues, for example, dangers of protection presentation, adaptability in key administration, adaptable access, and effective client disavowal, have remained the most critical difficulties toward accomplishing fine-grained, cryptographically upheld information get to control. In this paper, we propose a novel patient-driven system and a suite of instruments for information get to control to PHRs put away in semitrusted servers. To accomplish fine-grained and versatile information get to control for PHRs, we influence trait based encryption (ABE) systems to scramble every patient's PHR document. Unique in relation to past works in secure information re-appropriating, we center around the different information proprietor situation, and partition the clients in the PHR framework into numerous security spaces that enormously decreases the key administration intricacy for proprietors and clients. A high level of patient security is ensured all the while by misusing multiauthority ABE. Our plan additionally empowers dynamic alteration of access approaches or record traits, underpins proficient on-request client/quality repudiation and break-glass access under crisis situations. Broad scientific and exploratory outcomes are displayed which demonstrate the security, versatility, and productivity of our proposed plan.

III. PROPOSED SYSTEM

In our proposed system we are going to see about the four important concepts such as PHR, cryptography, cloud storage, Micro aggregation. A PHR set is the union of data records of the patients. Patients are considered to be owners of data and it should be stored securely in cloud. Similarly owners will encrypt their data before outsourcing it to the cloud. To encrypt the data ABE algorithm is used. Therefore cryptographic systems that require a pair of different keys to operate: one key (the public key) is used to encrypt messages and, the other key (the private key) is used to decrypt them.

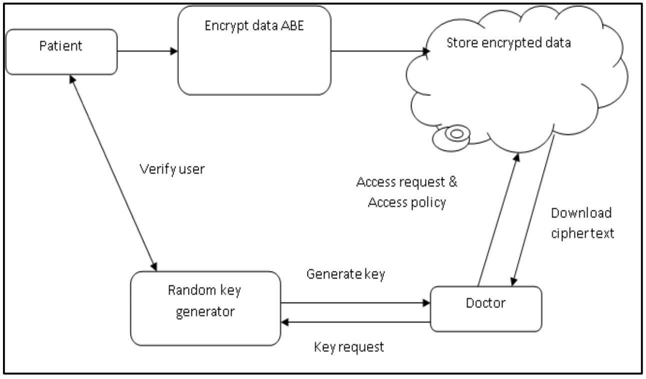

Fig. 1: System Architecture

Once the Cloud storage receives the patients' data, it checks the healthcare center ID of each message and forwards it to right Healthcare Center. Note that the cloud cannot access to the raw data of the patients because it is encrypted with the public key of Healthcare Center. Thanks to the use of their private key, each healthcare center can decrypt and access the raw biomedical data of the patients for which they are responsible. Doctors can analyze the complete data and decide on the proper procedures and protocols to apply without any information loss. We assume that healthcare centers are trust When the cloud receives the micro aggregated data sets from all healthcare centers, it merges them all and micro aggregates them again by using again a micro aggregation algorithm.

A. Implementation

1) Patient Login:

First the patient/user needs to login the account. If he doesn't have account he has to register. During registration the random key is set in order to enhance more security. Once username and password matches with the database then particular patient can login to next form. Here he/she enters his/her complete biomedical data. These data are encrypted using the encrypt key. Later it is aggregated and that data is sent to cloud.

2) Patient Description:

The patient will enter the details of his/her in the storage area. Using the file key the patient will encrypt the data and send to the cloud. The required file will be transferred to the doctor. ABE algorithm is also known as symmetric cryptography, refers to cryptographic systems that require a pair of keys to operate: one key (the public key) is used to encrypt messages and, the other key (the private key) is used to decrypt them.

3) Random Key Generation:

The doctor can download particular report of patient by satisfying attributes of owner of report. The patient will give the file to the doctor using the file key of decrypted data. So that the data will be fully secured and no one can able to access the file without the authentication key and the file key. After the patient sent the file, the doctor will receive the file. The doctor must open the file by sending the key request to the patient. After the patient viewed it, he/she can update the random key and the patient will send the original key to the doctor. With the authentication key and file key the doctor will process the file.

4) File Accessing by Doctors:

Here the data received from the client are accessed by the doctor by login to his account. The process is further preceded by requesting a random key to the patient. When the patient receives the message he sends the key to the doctor. The doctor accesses his required patient's details on successful matching of the key. Then the decrypted data is loaded initially. Then particular report is analyzed and prescription has been given by doctor and submitted to cloud. Once document is uploaded again accessing it using same accessing key is not possible. Therefore for every time accessing the file random key is generated and it should be matched to view the document.

5) Advantages:

– Security is enhanced due to the use of RC4 algorithm.
– Memory storage will be reduced.
– Processing time will be less.
– Improved micro aggregation for storage efficiency.

IV. RESULT AND DISCUSSION

Securing personal health records in cloud has been implemented. In this section the securing level of reports has been shown in figure 2.

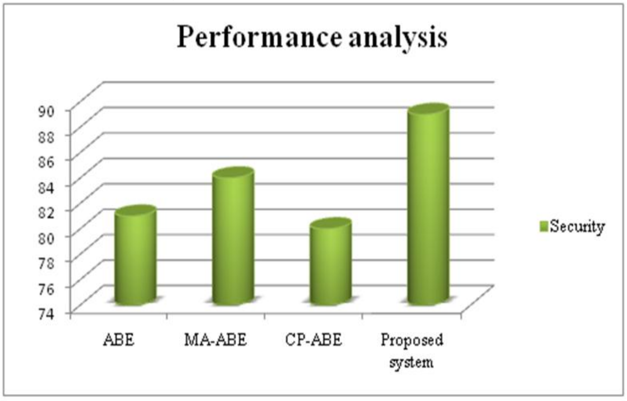

Fig. 2: Comparison of various encryption algorithms with our proposed system

V. CONCLUSION

The objective of our work is to store our PHR data in secure way in cloud and enabling secure data retrieval of data. Hence we achieve our objective by encrypting our data using ABE and storing it in cloud. Then again encrypting the file for providing higher security an access key policy is generated through Random Key Generator. Once patient entered their personal reports, the next updating process will be done by doctor. Whenever doctor wants to access particular patient file, he must need access key to download encrypted file. This key is not constant and it varies for every time. Then the file key is needed to decrypt the report and respective file will be accessed by doctor.

REFERENCES

[1] Sabna A B and Harsha T D, "Secure Sharing of Personal Health Records in Cloud Computing using Encryption" International Journal of Computer Applications Technology and ResearchVolume 4–Issue 1, 58-62, 2015, ISSN:-2319–8656.

[2] JianghuaLiu, XinyiHuang and Joseph K.Liu, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption" Future Generation Computer Systems Volume 52, November 2015, Pages 67-76.

[3] Satheesh.K and Ram kumar.A, "Scalable And Secure Sharing Of Personal Health Records In Cloud Computing Using Multi Authority Attribute-Based Encryption" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 1, March 2014.

[4] Rakesh. B and Harsha Vardhan. A, "Sharing Of Personal Health Recordsin Cloud Computing" Int. Journal of Engineering Research and Applications Vol. 3, Issue 6, Nov-Dec 2013, pp.1769-1773.

[5] Ming Li ; Shucheng Yu ; Yao Zheng ; Kui Ren ; Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption” IEEE Transactions on Parallel and Distributed Systems Volume: 24 , Issue: 1 , Jan. 2013.

[6] K.D. Mandl, P. Szolovits, and I.S. Kohane, “Public Standards andPatients’ Control: How to Keep Electronic Medical RecordsAccessible but Private,” BMJ, vol. 322, no. 7281, pp. 283-287,Feb. 2001.

[7] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “PatientControlled Encryption: Ensuring Privacy of Electronic MedicalRecords,” Proc. ACM Workshop Cloud Computing Security(CCSW ’09), pp. 103-114, 2009.

[8] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,”Proc. IEEE INFOCOM ’10, 2010.

[9] C. Dong, G. Russello, and N. Dulay, “Shared and SearchableEncrypted Data for Untrusted Servers,” J. Computer Security,vol. 19, pp. 367-397, 2010.

[10] Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,”Proc. 13th ACM Conf. Computer and Comm. Security (CCS ’06),pp. 89-98, 2006.

[11] M. Li, W. Lou, and K. Ren, “Data Security and Privacy in WirelessBody Area Networks,” IEEE Wireless Comm. Magazine, vol. 17,no. 1, pp. 51-58, Feb. 2010.

[12] Boldyreva, V. Goyal, and V. Kumar, “Identity-Based Encryptionwith Efficient Revocation,” Proc. 15th ACM Conf. Computer andComm. Security (CCS), pp. 417-426, 2008.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,“ Ciphertext-Policy Attribute-Based Threshold Decryption withFlexible Delegation and Revocation of User Attributes,” 2009.

[14] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based DataSharing with Attribute Revocation,” Proc. Fifth ACM Symp.[1] Information, Computer and Comm. Security (ASIACCS ’10), 2010.