Research on Privacy Preserving Models for Efficient Healthcare Big Data Sharing in Cloud

Suguna. M, Prakash D, Shobana G

ABSTRACT--- Healthcare data is highly confidential and thus sharing of those data is complex. But to diagnose a patient, the professionals need to access their healthcare data. Those data will be in the form of Electronic Medical Record (EMR) which includes multimedia data like X-ray, Scan and ECG. Size of the EMR is rapidly growing thus it is to be stored in format of Big Data. Major issue in Big Data is privacy, as EMR is taken into account a tiny change in data could create a larger impact. Data theft attack is considered to be the serious security breaches of Big Data. On the other hand, limiting the access of EMR must not restrict the data flow within the authorized users.

Keywords: Electronic Medical Record (EMR), KP-ABE algorithm, Big Data

I. INTRODUCTION

Every data across the world is converted into digital formats. This leads to the entry of digital technologies into the medical sector. As a result both health care data and patient data in clinical models have been digitalized. This improvement is greatly supported by the usage of variety of software in hospitals, increase in the number of mobile device users, consulting of doctors over the world through fast internet. Increase in size of health care data has paved the way to make use of Big data analytics. Usage of this technology brings lot of improvements in the healthcare sector but there are some issues and challenges in maintaining them. This move from responsive to proactive social insurance can result in progressed nature of consideration, decline in human services costs, and in the end lead to monetary development. For example, continuous remote checking of crucial signs through inserted sensors (appended to patients) permits human services suppliers to be alarmed if there should arise an occurrence of an oddity. These issues and challenges were becoming stronger nowadays. In addition, healthcare organizations found that a highly responsive, so they use technology-centric approach for detecting the security and privacy requirements but it is not enough to protect the medical data and its patients. Motivated thus, organizations have moved in the development of new security mechanisms to prevent the sensitive medical data being accessed or misused. In this paper we discuss some related works, the risks to the big health data security and some latest technologies to cover these risks. Lastly, we offer conclusions and highlight the future directions.

Revised Manuscript Received on August 14, 2019.

Suguna.M, Assistant Professor, Department of CSE, Kumaraguru College of Technology, Coimbatore, T.N, India. (suguna.m.cse@kct.ac.in)

Prakash D, Research Scholar, Anna University, Chennai, T.N, India.

Shobana G Assistant Professor, Department of CSE, Kumaraguru College of Technology, Coimbatore, T.N, India.(shobana.g.cse@kct.ac.in)

II. LITERATURE REVIEW

[1], describes when authenticated user attempt to access the system by giving an input, the source will not directly reach the server. The system maintains two tables to regulate the authentication which includes index table and privacy table. Index table has only the basic patient details that can be allowed to access publicly. Privacy table contains the medical data about the patients that will be accessed using a private key. Private Key is given only to the authorized user like organization head, consulting doctor or patient. Patient will not be allowed to edit the medical data in private table. This makes both the data will be available to public and also the patient details will be secured.

[2] define when using a single index table for storing large data it causes distortion of patient health data. This causes the data loss and also allows unauthorized users from accessing them. The idea behind the paper is to use two index tables such that mapping of input data to patient data will remain accurate. One table is named as alpha table that contains the identification of the mapping data of patients. Another is beta table that maps the identification with the patient data. These tables are not dependent with each other. Map reduce technique is used to produce a better and an optimal result when using two index tables.

[3] explains an optimal way to access the healthcare data by using a keyword search. Keyword is generated by the patient or the authority responsible to maintain the healthcare data. Keywords are to be unique and privacy comes into a main role. Generally keywords are generated and are used directly to search a incidence of data but in this paper keyword is encrypted after generation. The user requesting to view their health record must use the encrypted keyword that is again reencrypted by the proxy. Encrypting the keyword twice will protect the keywords from attackers as keyword does not remain the same.

[4] deals with a healthcare model designed for smart cities where social network is used along with the healthcare data to analyse the healthcare reports. Providing access of health data in social network remains as a great challenge to privacy aspects. There is high Possibility of data being modified and addition of corrupted data. Both Health data and social data are encrypted separately. The resultant cipher text is given to the users for accessing the data. Users can be healthcare providers as well as social users. Data can

be added even by using various sensors into the cloud for analysing.

[5] proposes the mechanism used to access the secured data. Generation of key remains as main phase to balance the security issues. An algorithm known as KP-ABE is used to generate the key for accessing the data. It can be expanded as key policy attribute based encryption, which deals with using certain attributes to generate the key. Uniqueness of the key is the drastic advantage of using this technique as individual attributes of the system is considered during key generation. These key could be again verified using attributes listed in the system.

[6] defines the prevention of hacker accessing health data using profile matching techniques. When the access request is given to the server, a unique token is generated and send to the requestor. The requestor must handover the token to the content manager. Work of content manager is to verify both the token received and the profile that has sent the request. Profile match is found only if the request is from the authenticated user. After verification the content manager would forward the requested data to the user. In this paper various factors like profile aspects, token, user request were verified before providing access to data this increases the efficiency of privacy preserving.

[7] proposes solution to deal with the keyword guessing attack. Keywords are shared to the users of the data. The keywords can be easily guessed and are made available for attack by the hackers. To overcome that designated tester is used to check the keywords. The system without tester returns the data only by using the keywords searched it can be done by unauthorized user also. In this paper a checker will enable data only to the registered or authorized users.

[8] describe the variation in storage spaces every time the data is updated. As the patient enters his medical data in cloud it will be shared in a server and maintained there. Hacking of data from that server could bring a great threat to privacy concern. In this paper the data is stored in various cloud servers every time the data is updated. This paves the way for a multiple cloud provider. Maintaining of patient history is the great challenge in this system as there is a constant shift in the cloud provider.

[9] Component configuration is a sub-field of microeconomics also, amusement hypothesis. It thinks about how to actualize great framework wide answers for issues that include different self-interested specialists with private data about their inclinations for various results. Fusing system

Plan into the investigation of security ensuring has as of late pulled in some consideration. More or less, an instrument denes the procedures accessible and the strategy used to choose the nal result dependent on specialists' systems.

[10] This task gives a security to the social insurance records of the patients that are put away in the cloud. This application can be extremely helpful amid the crisis situations where the past wellbeing record of the patient is required. For every one of the approved clients has been empowered with Proxy re-encryption work in E-wellbeing cloud so as to keep the abuse of information by the attackers. With the assistance of irregular different catchphrases the pursuit task can be performed to get to the information and intermediary server will help to unscramble the scrambled information if the client has the substantial day and age gave. Further this application can be utilized for some approved client in future. Furthermore, some extra forms of the application can be included and utilized. The capacity of the information is secure and broadly utilized in the medicinal services applications.

[11] huge information changes human services, security of patient information is vital in medical field to get advances. The medicinal services mists has enormous information wind up noticeable, facilitating organizations will be progressively hesitant to share gigantic human services information for brought together handling. Henceforth, we imagine appropriated preparing crosswise over different mists and utilizing on aggregate insight. Secure patient information the board is inescapable as human services mists total what's more, connect a lot of information from dissimilar systems. Moreover, secure and protection saving constant

investigation will drive proactive social insurance and health.

III. METHODOLOGY & RESULTS DISCUSSIONS

It is assumed that KP-ABE algorithm could be combined along with data sharing to overcome the security issues. Doctors can enrol their data in server by giving their personal information, medical practice certificate number. After they registered, they have to wait for some time until their registration is accepted by administrator or higher officials like administrator or dean of doctors committee. After their registration is accepted by administrator, they can log into the server by giving their user id and password. After that they have to give a secret key which is generated and sent by administrator. Here, Administrator has to be approved /reject the doctor's application based on their certificate and practice term. Whenever a doctor is logged in, a unique and secret key is generated based on KP-ABE technique for him by administrator. All the personal and health information are registered by a doctor who is taking care of the patient initially. After the registration process, one time unique id is generated for that patient. This id is informed by doctor to the patient either by in person or through mail id or mobile number. Regarding health information, doctor has to give blood pressure, blood test report, scan report, ECG report and lot if they have any other information about patient's health. Once patient's information is registered in the server, he can go to any doctor in the world for the treatment. First, patient has to give his patient id to the doctor who is going to take the treatment for him at present. After that his previous health information, treatment, doctor name, previously taken medicine are accessed from the server and shown on doctor's screen. And then the doctor has to add the medicine details which is prescribed by him and he can add the scan reports, ECG reports, surgery details and other test reports. Patient also can view his personal and health information by giving his patient id and finger print. Fingerprint of the

existing users are verified before new users are registered. If the finger print already exists, an error message is send to the new user. If new finger print does not match any of the available fingerprint registration will be completed, by this way replication will be avoided.

IV. CONCLUSION

Among the proposed systems discussed in this paper that can protect the privacy of clients and the intellectual property of Health service providers usage of KP-ABE technique remains effective. Since patient health information's are maintained in the server individually their PHR couldn't be lost. So health records can be only accessed by authorized users. To conclude, for small companies with security constrains, this design helps them to reduce the burden by applying KP-ABE.

REFERENCE

1. Efficient Privacy preservation techniques for maintaining healthcare records using big data, S.Jegadeesan, S.Pooja, T.Vidhya, of 2016 International Journal of innovative research in computer and communication Engineering
2. Hybrid privacy preservation framework for healthcare data publishing, Kingsford Kissi Mireku, Zhang FengLi, Kittur Philemon kibiwott, of 2017
3. Conjunctive Keyword Search with designated tester and timing enable proxy re-encryption function for E-health cloud, yang yang, maode ma, of 2012 IEEE transaction on information forensics and security
4. Secure and privacy-Preserving Data sharing and collaboration in Mobile Healthcare Social Networks in Smart cities, Qinlong Huang, Licheng wang, Yixian yang, of 2017 Hindawi security and communication networks. american journal of engineering research.
5. Efficient Verifiable Public Key Encryption with keyword search based on KP-ABE, Pengliang Liu, Jianfeng wang, Hua Ma, Haixin Nie, of 2014 Ninth International Conference on Broadband and Wireless Computing
6. A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data, Wwnyi Liu, A. Selcuk Uluagac, Raheem Beyah, of 2012
7. An enhanced searchable public key encryption scheme with a designated tester and its extensions, chengyu Hu, pengtao Liu, of 2012 Journal of Computers, Vol. 7, No.3
8. Secret sharing for health data in multi-provider clouds, Tatiana Ermakova, Benjamin Fabian, of 2017 IEEE International conference on Cloud Data sharing
9. Information Security in Big Data: Privacy and Data Mining, lei xu, chunxiao jiang, jian wang, jian yuan, yong ren, IEEE – 2014
10. Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption in Health Cloud, Soumiya Y Patil Archana J. N, IJIRST-2017
11. Big data security and privacy issues in healthcare**,** Harsh Kupwade Patil and Ravi Seshadri, 2014 IEEE International Congress on Big Data