iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** XII **Month of publication:** December 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

Methodical Privacy Preservation Proficiency on Medical Records

P.Jayaselvi[1], M. Padma Priya[2], G. Jayanthi[3]
[1,2]*Department of Computer Science and Engineering, Sri Sairam Engineering College, Chennai, India*
[3]*Department of Instrumentation and control engineering, Sri Sairam Engineering College, Chennai, India*

Abstract*: Stored information and encryption keys are usually managed by the cloud provider. This data's can be easily hacked by the intruder. In order to overcome this we propose a proxy re-encryption technique which performs a two level encryption before storing the actual data into the cloud. A PROXY RE-ENCRYPTION plays a major role in maintaining sensitive information while maintaining the efficiency and reliability of stored data. Here we use two server one local and another cloud server and we also use two encryption keys called index level and privacy level. Index key are managed by the cloud server as it is less secure and contains searchable keywords only whereas privacy key are managed by the local server and it is more secured because only the data owners can have access to confidential information. Here we have developed an android application for the convenience of the inpatients and outpatients. Using the application, patients can register for an appointment and can get a token before going to the hospital. Patients can view the prescription information recommended by the doctor from our mobile application.

Keywords: proxy server, encryption, privacy, healthcare, big data.

I. INTRODUCTION

The technology development in healthcare bigdata and wearable technologies as well as the cloud computing technologies, cloud-assisted healthcare bigdata computing has become complex to meet the users ever growing needs on health consultation. However it is a challenging problem to personalize health care data specifically for various uses in a convenient fashion. Previous work has suggested that the integration of healthcare services and social network scan be used to retrieve the real time information about the diseases which will be helpful to simplify the treatment process.

In a healthcare social platform patients can obtain data by sharing themselves with other similar patients. Even though both doctors and patients has been benefitted by sharing the medical data but if the sensitive and private data gets stolen or leaked it can cause security problem. This happens when there is no protection mechanism applied to secure the shared data. As cloud computing is advancing, a huge amount of data can be stored in various clouds such as remote clouds and cloudlets which felicitates sharing of data and complex computations.

However data sharing in cloud faces some problems such as how to preserve the privacy of patient's health information during its delivery to a cloudlet, how to confirm that sharing data in a cloudlet will not cause any privacy and security problems and also how to effectively preserve the system from malicious attacks and finally how efficiently the user can access their healthcare information from the cloudlet.

In order to overcome the above problems we propose a cloud based healthcare system in which the data's from patients body are collected using a wearable deviceand then the data's are transmitted to the nearest cloudlet and finally those data's are sent to the remote cloud where the doctors can make use of those data for diagnosing the diseases. The privacy protection has been separated into three stages based on the delivery of data. In the first stage we are using two level of encryption instead of single level encryption for privacy and in the second stage we are using two servers, one is cloud server for storing index key and another one is local server which is used to hold the privacy key. In the third stage we are implementing an android application interface over here for the efficient access of the users called 'inpatients' and 'out patient's for their health care description.

II. RELATED WORK

Rongxing Lu et al [3] proposed an efficient and privacy-preserving aggregation scheme, named EPPA which is used for smart grid communications. EPPA uses homomorphic Paillier cryptosystem technique to structure multidimensional data and encrypt the structured data. For data communications from user to smart grid operation centre, at local gateway without decryption data aggregation is performed direct on cipher text, and the aggregation result of the original data can be obtained at the operation centre. To reduce authentication cost EPPA also adopts the batch verification technique. EPPA lowers the computation cost and

communication overhead, and also it protects user privacy and it prevents from various security threats. But it provides less security and not much efficient on large amount of data.

Rongxing Lu et al [2] proposed a secure and privacy-preserving opportunistic computing framework called SPOC for mobile healthcare emergency. Here with minimal privacy disclosure, the smart phone resources can be used to process personal health information (PHI) during m-Healthcare emergency. It uses a User-centric privacy access control which helps to detect who can participate to assist the processing of overwhelming PHI data. In addition, performance evaluations via extensive simulations demonstrate the SPOC's effectiveness in providing high-reliable-PHI process. But in SPOC Cost requirement is high in dealing with the medical records.

Min Chen et al [1] says that traditional healthcare system often requires the release of medical reports to the cloudlet. For collecting data it uses the Number Theory Research Unit (NTRU).The input data is collected from the wearable device and then the input is encrypted by this NTRU method and that information will be sent to the nearest cloudlet. Secondly, it helps users to select secure partners who all want to share the information through cloudlet. Thirdly it divides user's medical data stored in remote cloud and gives the proper preservation. At last a collaborative intrusion detection system (IDS) method had been developed based on cloudlet mesh in order to secure the healthcare system from malicious attacks,. The major drawback in this is Intrusion avoidance is not possible.

III.EXISTING SYSTEM

Many industrial data's are being stored in a cloud and we cannot predict whether all the stored data are secured, hence all the stored data's are encrypted. Existing System uses Similarity check Protocol for search over the Encrypted data. It takes longer time to search over encrypted data because the entire stored document must be decrypted before starting the comparison process. All stored patient information is encrypted using the same public key so it's less secure. We can also run operations over encrypted data to protect individual Privacy in data analytics. However, as operations over encrypted data are usually complex and time-consuming, while the data is of high-volume and needs us to mine new knowledge in a reasonable timeframe. Cloud providers may break all information because they manage most of the encryption key. Also there is no secure mobile application for outpatient interface.

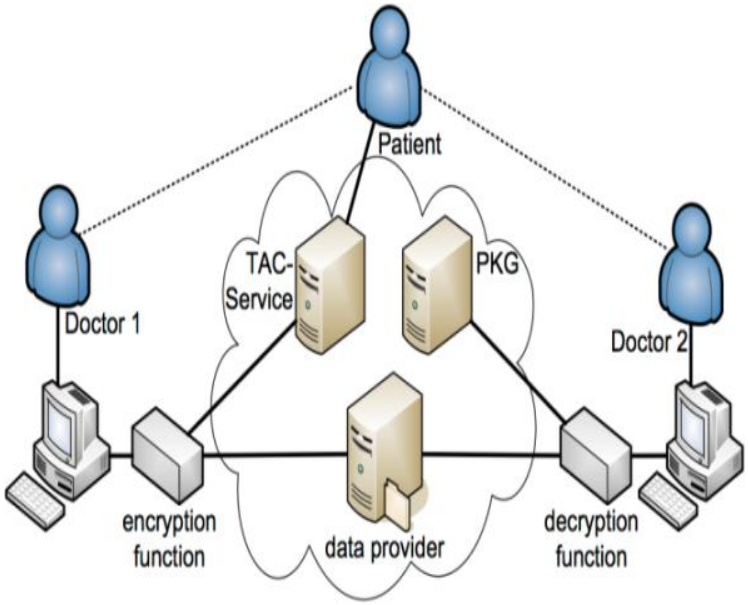


Fig. 1General Block diagram

IV.PROPOSED SYSTEM

In proposed system we introduced novel concept "two level encryption" for that we uses DES algorithm and linear congruential generator. All stored patient information has search index and privacy table. Search index contains only the keywords that are searchable since encryption keys are common to all patients. Network admin maintains the Privacy table which contains unique encryption key for all the patients. These keys only provide authorized request which means patient can set instruction to access the key. Here we develop an android application for outpatient interface, using this application patient can register our information and also get token before going to hospital. Patient can view our prescription information from our mobile application.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor :6.887
Volume 5 Issue XII December 2017- Available at www.ijraset.com

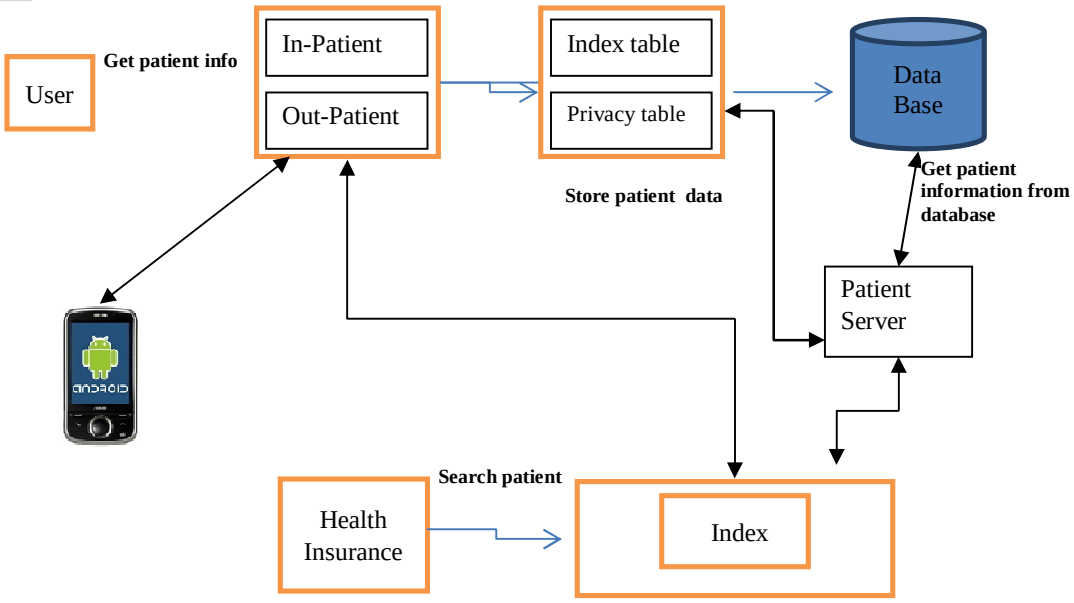


Fig. 2 Privacy preservation in Health care system

V. MODULES

Firstly a Client Interface Design is developed in which we have in Patient and outpatient menu to access patient relevant data's.For providing security services we implement two levels of encryption

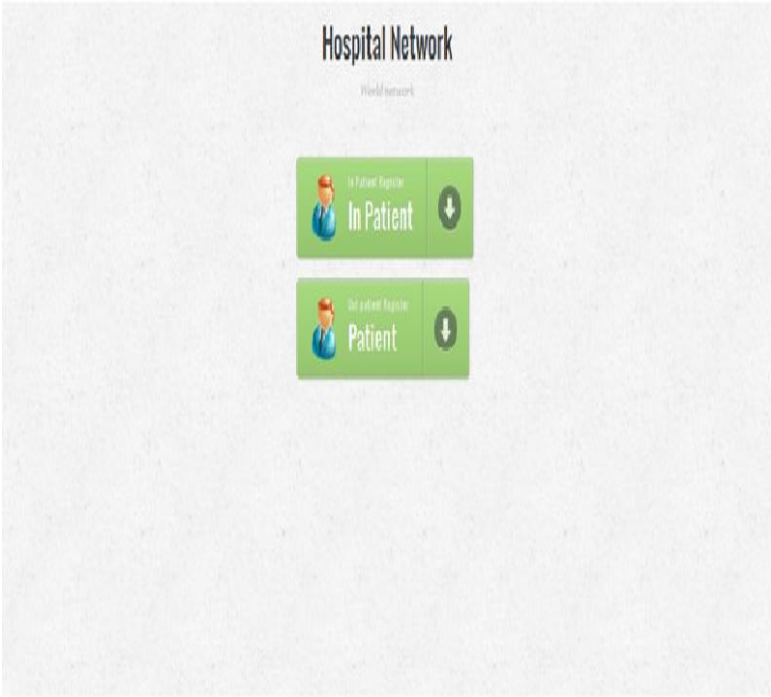


Fig.3 Hospital network for healthcare

A. First level Encryption

In this Module We implement First level Encryption. Firstly the patient registers and after the completion of registration, collected data's are divided into two classes: searchable keyword, personal Searchable keywords which are then stored in single level encryption format and personal information are stored in double level encryption

Level one encryption key are stored by cloud service provider in order to search specific user details.

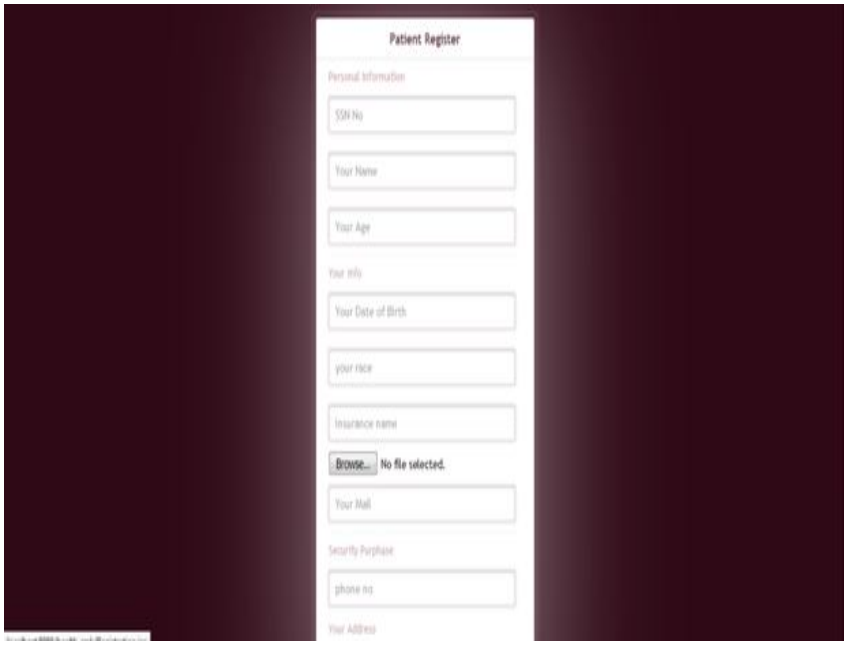


Fig.4 Patient registration form

B. Second Level Encryption

A Second level encryption key is generated when user submits the registration form and the generated keys are kept securely. This system has one frontend layer (called security layer) from which user can set criteria for accessing our key. Criteria can be of any type (ip,uid, security-key), this system provides second-level-encryption key. Uploaded data split into multiple parts each part is then encrypted using private key. Finally it is stored in Database server. For generating encryption keys two algorithms linear "congruential generator" and "DES" we have used.

C. Linear congruential generator

An LCG is essentially formula of the following form:

Number= (a * number +C) mod m

In other words we begin with some "seed" number which is ideally "genuinely unpredictable", and in practice is "unpredictable enough". Each time when we want a random number we multiply the current seed by some fixed number 'a'. Add another fixed number 'c' to the result then take the modulo of fixed number (m) to the result ant. The number a is generally large.

D. Data Encryption Standard Algorithm

DES is a block cipher in which a block of data is processed with a key and algorithm simultaneously rather than one bit at a time. While encrypting the plain text message, DES groups it into64-bitblocks. Each block is enciphered using the secret key into a64-bitciphertextusingan initial permutation. Decryption is nothing but the inverse of encryption which follows the same steps but keys are applied in reverse order.

E. Token Book and Prescription History

In this module we create an android application for outpatient access network server, from this application patient can register and also get token before visiting the hospital. This application uses GCM(Google cloud messaging) for communicating to the network server.GCM is effective server because that used Extensible Messaging and Presence protocol(Xmpp) which is light weight protocol so that we can avoid battery drain.

In prescription history module doctors can add prescription for patient reference. Information kept securely in cloud, for providing security to the data des algorithm is used.User can view prescription information from android application.

Fig.5 An android application for outpatient access network

VI.CONCLUSION

We have identified the privacy requirements related to the data and analysed the challenges in terms of privacy concern in a cloud environment and discussed whether existing privacy-preserving methods are sufficient for processing the data's. We have also proposed an efficient two-level encryption calledproxy re-encryption technique for maintaining sensitive information while maintaining the efficiency and reliability of stored datawhich thereby provides more security to the data stored in a cloud.Finally we have developed an android application for the convenience of the inpatients and outpatients.

REFERENCES

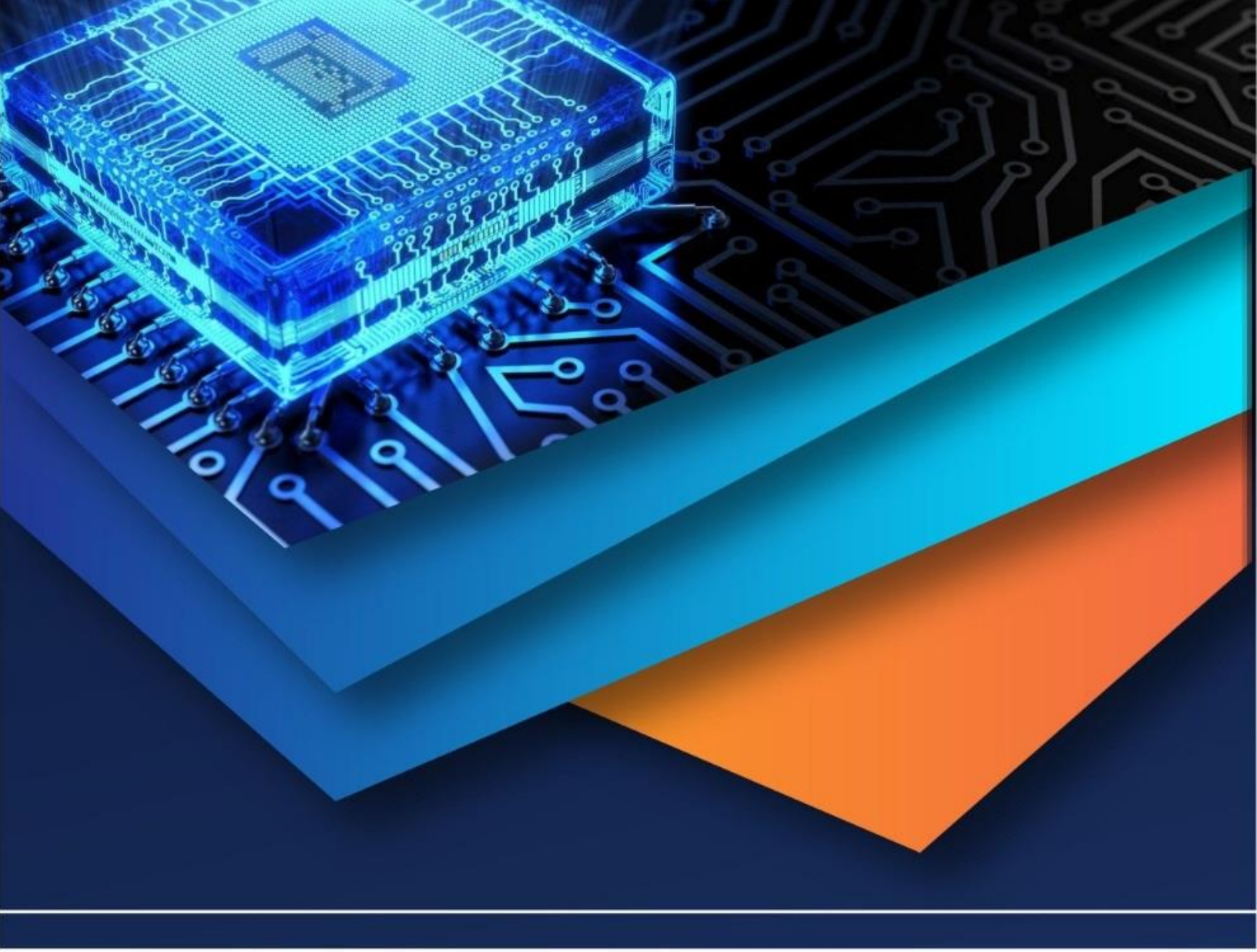
[1] Min Chen,YongfengQian, Jing Chen, Kai Hwang, Shiwen Mao and Long Hu."Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing" IEEE Transactions on Cloud Computing Volume: PP, Issue: 99 ,2016.

[2] Rongxing Lu, Xiaohui Liang, Xu Li, XiaodongLin andXuemin (Sherman) Shen, " SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency" IEEE Transactions on Parallel and Distributed Systems ,Volume: 24, Issue: 3, March 2013 .

[3] Rongxing Lu, Xiaohui Liang, Xu Li, XiaodongLin andXuemin (Sherman) Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications",IEEE Transactions on parallel and distributed systems Volume: 23, Issue: 9, Sept. 2012.

[4] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, "A security framework in g-hadoop for big data computing across distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[5] M. S. Hossain an G.Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring,"Computer Networks, vol. 101, pp. 192–202, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY