ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

An Efficient Secure Protocol for Storing and Retrieving Health Care Records in Cloud Environment

R.Nijanthan Balaji[1], P.Barani Rahul[2], K.Naveen Raj [3,] K.Balachandar[4]

B.E. Student, Department of CSE, Velammal Institute of Technology, Panchetti, Chennai, India[1,2,3]

Assistant Professor, Department of CSE, Velammal Institute of Technology, Panchetti, Chennai, India[4]

ABSTRACT: Proxy re-encryption is an intermediate server that improves efficiency, reliability and economical. It plays an importance role when in maintaining sensitive information. Before that, most of stored information data's, encryption keys are managed by cloud provider, so may possible to hack that info. In this project we proposed proxy re-encryption technique , it perform two level encryption before actual data store in cloud , for using this technique need two server one local server another cloud server. We propose two encryption key index level, privacy level. Index key are managed by cloud server because it is less secure, only contain searchable keywords, privacy key are managed by local server because it more secure only known by the data owner, contains all privacy information. We develop an android application for outpatient interface, using this application patient can register our information and also get token before go to hospital. Patient can view our prescription information from our mobile application. This system introduces emergency patient basic information retrieval in case of any panic situation through an android application with a unique id for each patient.

KEYWORDS: proxy re-encryption, index level, privacy level, in-patient, out-patient, DES

I.INTRODUCTION

Nowadays cyber security is one of the major constraint faced by several types of organization. In that case securing patient records in the hospital management system is the most important task. Mostly the organization like hospitals requires large amount of storage space, so they would prefer for cloud storage. Although various types of systems are existing for the process of storing the documents in the efficient manner, our proposed system will provide two level of encryption and two different secured methods of acceding the information. We propose two encryption key index level, privacy level. Index key are managed by cloud server because it is less secure, only contain searchable keywords, privacy key are managed by local server because it more secure only known by the data owner contains all privacy information. The aim main of our project is store the sensitive information in a secured manner in the cloud storage and also provide access for the user's basic information in the health records under critical situations and also secured access for the third party access for example insurance company. The main aim not giving the overall control to the cloud server some of the permissions are controlled by the local server.

II.RELATED WORK

An electronic health record (EHR) system is a novel application that will bring great convenience in healthcare. The privacy and security of the sensitive personal information are the major concerns of the users, which could hinder further development and widely adoption of the systems. The searchable encryption scheme is a technology to incorporate security protection and favourable operability functions together, which can play an important role in the e-health record system. In this paper, we introduce a novel cryptographic primitive named as conjunctive keyword search with designated tester and timing enabled proxy re-encryption function, which is a kind of a time-dependent SE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

scheme. It could enable patients to delegate partial access rights to others to operate search functions over their records in a limited time period. The length of the time period for the delegate to search and decrypt the delegator's encrypted documents can be controlled. Moreover, the delegate could be automatically deprived of the access and search authority after a specified period of effective time. It can also support the conjunctive keywords search and resist the keyword guessing attacks. By the solution, only the designated tester is able to test the existence of certain keywords. We formulate a system model and a security model for the proposed Re-dtPECK scheme to show that it is an efficient scheme proved secure in the standard model. The comparison and extensive simulations demonstrate that it has a low computation and storage overhead.

Most of the industrial data stored in cloud computing, but cannot predict all stored data must have secured, hence most of cloud data are encrypted Most of the encryption key are managed by cloud provider's, So provider's may break all information. In existing system using similarity check protocol for search over the encrypted data using this protocol we can take long time to search over encrypted data, because all the stored document must be decrypted before starting the comparison process. All stored patient information must encrypted same public key so less secure.
Xiaohui Liang has said in [7] has explained the concept of smart grid has emerged as a convergence of traditional power system engineering and information and communication technology. It is vital to the success of next generation of power grid, which is expected to be featuring reliable, efficient, flexible, clean, friendly, and secure characteristics. In this paper, we propose an efficient and privacy-preserving aggregation scheme, named EPPA, for smart grid communications. EPPA uses a super increasing sequence to structure multidimensional data and encrypt the structured data by the homomorphic paillier cryptosystem technique. For data communications from user to smart grid operation center, data aggregation is performed directly on cipher text at local gateways without decryption, and the aggregation result of the original data can be obtained at the operation center. EPPA also adopts the batch verification technique to reduce authentication cost. Through extensive analysis, we demonstrate that EPPA resists various security threats and preserve user privacy, and has significantly less computation and communication overhead than existing competing approaches.

Shucheng Yu; Kui Ren; Wenjing Lou has described the privacy assurance in cloud services in [3] such as Cloud computing is envisioned as the next generation architecture of IT enterprises, providing convenient remote access to massively scalable data storage and application services. While this outsourced storage and computing paradigm can potentially bring great economical savings for data owners and users, its benefits may not be fully realized due to wide concerns of data owners that their private data may be involuntarily exposed or handled by cloud providers. Although end-to-end encryption techniques have been proposed as promising solutions for secure cloud data storage, a primary challenge toward building a full-fledged cloud data service remains: how to effectively support flexible data utilization services such as search over the data in a privacy-preserving manner. In this article, we identify the system requirements and challenges toward achieving privacy-assured searchable outsourced cloud data services, especially, how to design usable and practically efficient search schemes for encrypted cloud storage. We present a general methodology for this using searchable encryption techniques, which allows encrypted data to be searched by users without leaking information about the data itself and users¿ queries. In particular, we discuss three desirable functionalities of usable search operations: supporting result ranking, similarity search, and search over structured data. For each of them, we describe approaches to design efficient privacy-assured searchable encryption schemes, which are based on several recent symmetric-key encryption primitives. We analyse their advantages and limitations, and outline the future challenges that need to be solved to make such secure searchable cloud data service a reality.

III.PROPOSED METHODOLOGY

In proposed system we introduced novel concept "Two level Encryption" for that we used linear congruential generator algorithm. Search index contain only searchable keywords, so that encryption keys are common to all patient. Privacy table are maintained by network admin that contains unique encryption keys for all patient. Those key only provide authorized request, that means only patient can set instruction for access for key, instruction can be of any type such as IP address or unique id. We developed an android application for emergency patient information access where patient will be provided with a unique id. Because suddenly if the patient met with accident or any kind of panic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

situation by using the unique id the doctor can get the treatment information, so that he can provide appropriate first aid for the patient

Two level encryption is the major key aspects of this system which provides high level of security of e-health records. Mobile interface have been introduced here for effective retrieval. Public key will be available for all, whereas the private key will be maintained by the network admin using the android application the patient can generate token before going to the hospital. At emergency situation the android app will provide a greater help for the doctors to know the patient information to provide appropriate first aid. Highly secure for the data than the existing system.

Client Interface:

In this module we develop interface page, in our project have two types of client hospital and insurance companies for access patient data's. For apply security service we implement two level encryption concept. Once server authentication process completed, we design patient info web port to get all necessary information about patient health report. Each patient uploaded document must be stored in own encryption key, which is known only to the user. And also create an android application for patient interface. This system maintain two type of patient information in-patient and out-patient. All request must be authenticated before going to patient database.

First Level Encryption

Inthis module we implement first level encryption once the patient registration process completed, that data are classified into two types they are searchable keyword and personal. Searchable keywords are stored in single level encryption format, another, personal info are stored in double level encryption First level encryption key are keep by cloud service provider for search specific user. A unique encryption key is generated once the authentication is matched. The key is generated by the linear congruential generator which provides a random values for encryption. Once it is matched, the request is forwarded to the patient server. The patient server is accessed by both the database and the insurance. It has an authentication check criteria which is the request will be accepted only based on some constraints (particular IP, hospital).

Second Level Encryption

Second level encryption key generate when user submits the registration form, that keys are keep securely in network admin system. That system has frontend layer (security layer), using this layer user can set criteria for access our key. Criteria can any type (ip, uId, security-key) this system provide second-level-encryption key only satisfy request criteria. After the authentication is matched a privacy key will be generated. Only using this privacy key the database can be accessed else it cannot be accessed, so the database is completely authenticated. It decrypts the documents of the patient from the database. The documents will be shown only visible who is requesting the information i.e. either the hospital or insurance

Android App

We developed an android application for emergency patient information access where patient will be provided with a unique id because suddenly if the patient met with accident or any kind of panic situation by using the unique id the doctor can get the treatment information, so that he can provide appropriate first aid for the patient.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

IV.SETUP AND RESULTS

Given Below we have provided the setup of the portal

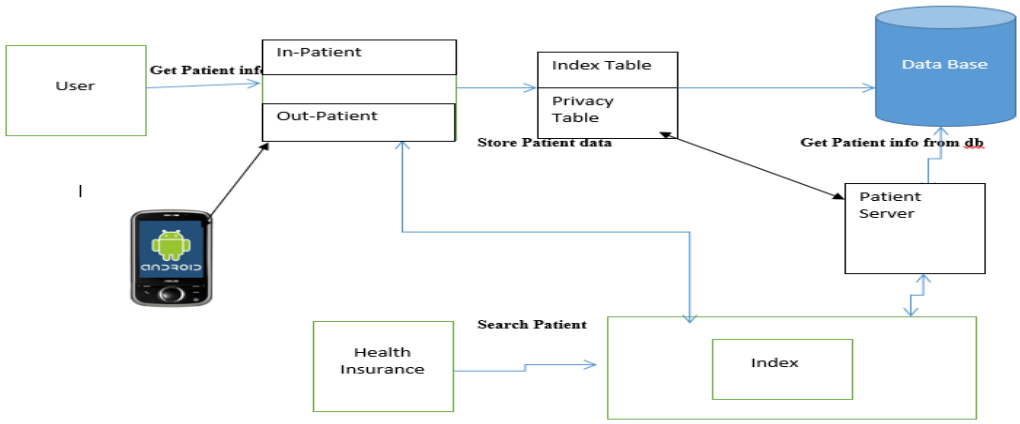

Fig 1: Overall Architecture Diagram

During this process the patient can register through the in-patient interface and get their data encrypted using two levels of encryption. One public key will be handled by the cloud server and private key will be maintained by the data owner. Patient server will handle the private key which encrypt the data in the privacy table, if the health insurance agent needs to access the patient info he will request the user and the particular doctor connected to the patient record will receive an notification and process the request by generating an OTP to the insurance agent to access the patient data

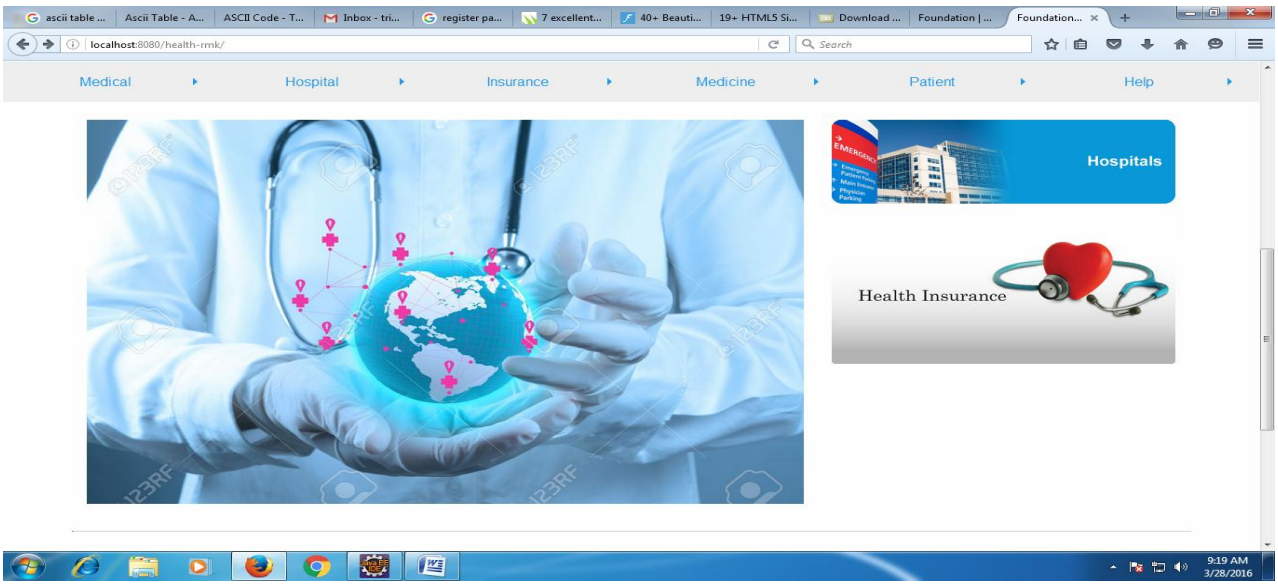

Fig 2: Index Page

The above Fig 2 displays the web apps which are availale in the portal, it provides access to all the end users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

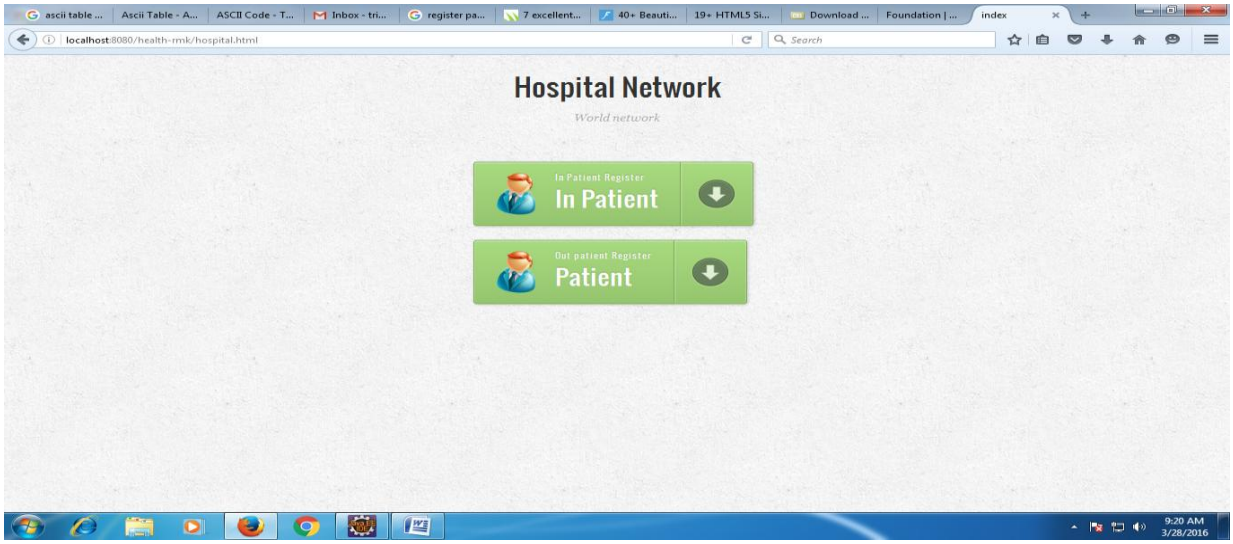

Fig 3: Index page

Also we proposed two new component "inpatient" and "outpatient" both patient information are stored in two level encryption format. Through inpatient the patient will register their data in the database in that patient data will be separated into index level and privacy level

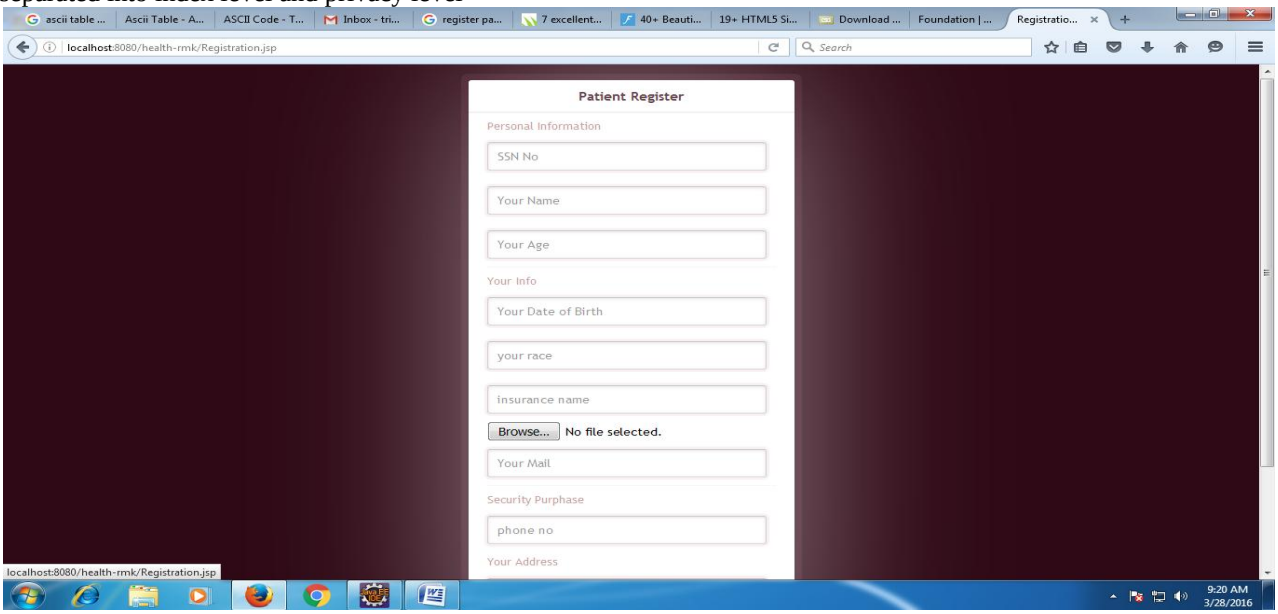

Fig 3: Patient registration form

Here the patient register their data details in the web portal which will be available through the inpatient interface. After storing the data searchable keywords will be stored in the index table and sensitive information will be stored in the privacy table and encrypted using DES algorithm and the private key will be stored in the patient server who is the data owner.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

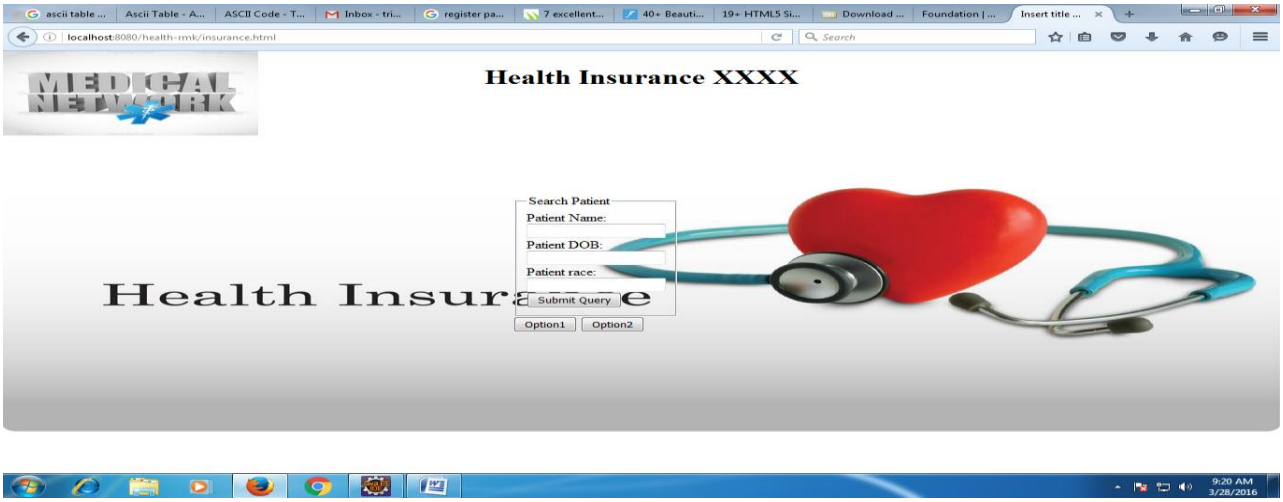

Fig 4: Health insurance page

Through this page the health insurance agent can search for the required patient data in the database. The doctor will enter the patient basic info like name, dob and race through this a notification will be sent to the doctor who is connected to the patient server and an OTP will be generated and sent to the health insurance agent who is requesting the patient data.

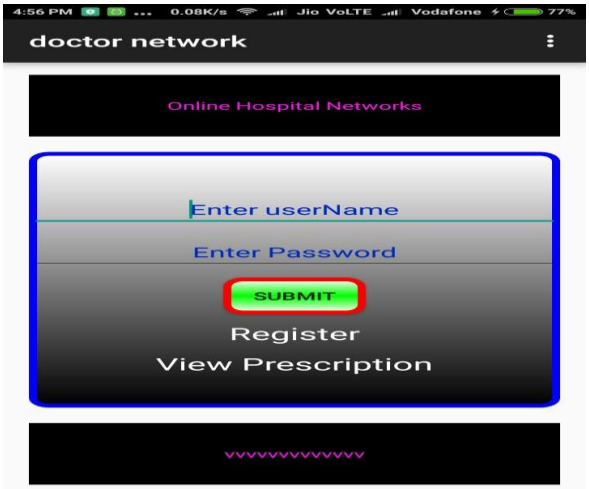

Fig 5: Android app homepage

We develop an android application for outpatient interface, using this application patient can register our information and also get token before go to hospital. Patient can view our prescription information from our mobile application. In this project introduced emergency patient basic information retrieval in case of any panic situation through an android application with a unique id for each patient.

V. CONCLUSION

In this article, we have investigated the privacy challenges in the Cloud computing by first identifying the data privacy requirements and then discussing whether existing privacy-preserving techniques are sufficient for data processing. We

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

have also introduced an efficient and privacy-preserving Two-level encryption in response to the efficiency and privacy requirements of data mining in the cloud

ACKNOWLEDGEMENT

We are extremely thankful to our Vice Principal Prof.Dr.S.Soundararajan and grateful to our Head of the Department Mrs.S.Selvakanmani, our librarian Mr.V.R.Murugan and our project coordinator Mrs.A.V.Kalpana, Computer Science and Engineering for their moral support. We would like to convey our sincere thanks to our guide Mr.K.Balachandar for his constant technical support and stupendous encouragement, which enabled us to complete our project successfully.

REFERENCES

[1] IBM, "Big Data at the Speed of Business," http://www-01.ibm.com/software/data/bigdata/, 2012.
[2] X. Wu et al., "Data Mining with Big Data," IEEE Trans. Knowledge DataEng. vol. 26, no. 1, 2014, pp. 97–107.
[3] S. Liu, "Exploring the Future of Computing," IT Professional, vol. 15, no.1, 2013, pp. 2–3.
[4] Oracle, "Oracle Big Data for the Enterprise," http://www.oracle.com/caen/technologies/big-data, 2012.
[5] "Big Data at CSAIL," http://bigdata.csail.mit.edu/.
[6] R. Lu et al., "EPPA: An Efficient and Privacy-Preserving Aggregation Shemefor Secure Smart Grid Communications," IEEE Trans. Parallel Distribution. Sys. Vol. 23, no. 9, 2012, pp. 1621–31.
[7] P. Paillier, "Public-Key Cryptosystems based on Composite Degree Residuosity Classes," EUROCRYPT, 1999, pp. 223–38.
[8] M. Li et al., "Toward Privacy-Assured and Searchable Cloud Data Storage Services," IEEE Network, vol. 27, no. 4, 2013, pp. 1–10.
[9] A. Cavoukian and J. Jonas, "Privacy by Design in the Age of Big Data," Office of the Information and Privacy Commissioner, 2012.
[10] R. Lu, X. Lin, and X. Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency,"
[11] J. W. Byun and D. H. Lee, "On a security model of conjunctive keyword search over encrypted relational database," J. System. Software., vol. 84, no. 8, pp. 1364–1372, 2011.
[12] M. Ding, F. Gao, Z. Jin, and H. Zhang, "An efficient public key encryption with conjunctive keyword search scheme based on pairings," in Proc. 3rd IEEEInt. Conf. Network. Infrastructure. Digit. Content (IC-NIDC), Beijing, China, Sep. 2012, pp. 526–530.
[13] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," Inf. Sci., vol. 180, no. 13, pp. 2576–2587, 2010.
[14] W.-C. Yau, R. C.-W. Phan, S.-H. Heng, and B.-M. Goi, "Proxy re-encryption with keyword search re-encryption with keyword search: New definitions and algorithms," in Proc. Int. Conf. Security Technol., vol. 122. Jeju Island, Korea, Dec. 2010, pp. 149–160.
[15] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-cipher text secure anonymous conditional proxy re-encryption with keyword search," Theoretical Computer Sci., vol. 462, pp. 39–58, Nov. 2012.

BIOGRAPHY

P.Barani Rahul is a final year student,CSE department in Velammal Institute of Technology(Affiliated to Anna University,Chennai). His research interests are Cloud Computing and Big Data.

Naveen Raj is a final year student,CSE department in Velammal Institute of Technology(Affiliated to Anna University,Chennai). His research interests are Cloud Computing and Database.

R.Nijanthan Balaji is a final year student, CSE department in Velammal Institute of Technology(Affiliated to Anna University,Chennai). His research interests are Cloud Computing and Artificial Intelligence.