ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Secured Health Records Storage & Retrieval System Using Keyword Based Key Generation and Attribute Based Encryption (ABE).

Morusu Rahul Reddy, Anusha N* and Naga Vishnu Shankar B

Department of Computer Science and Engineering, Sathyabama University, Chennai, India.

ABSTRACT

Storing the Personal Health Records (PHR's) manually in database takes lot of time and is also not secure. Due to massive growth of health domain makes this process more tedious. In this paper, a method is proposed where the information of the patient can be stored in the cloud environment. User files are automatically placed in the public & private cloud based on the sensitiveness of the data. Normal files are placed in the public cloud, where as critical data is placed in the private cloud. The data is stored in multiple servers for fast data retrieval by using Attribute Based Encryption (ABE). When user's access is manipulated, the intimation is given to the authorized users through the web page for security based data access. OTP (One Time Password) is generated by the help of Keyword Based Key Generation to the authorized users via email for security based data access to cross the attribute of user privilege to deploy cross privilege access via android mobile. With proposed method security level is increased and the trust worthiness is also maintained.

Keywords: ABE (Attribute Based Encryption), OTP (One Time Password), Public cloud, Private cloud, Keyword Based Key Generation

****Corresponding author***

INTRODUCTION

Healthcare services need quick access to health data which helps in saving life by assisting timely treatment in medical emergencies. Electronic healthcare system plays a very important role in human life. Technologies that are supported by mobile devices, such as home care and remote monitoring, make patients to retain their living style and cause negligible interference to their day by day exercises. The clinic inhabitance will be diminished consequently, permitting patients with higher need of in-healing center treatment to be conceded. Individuals got to be mindful that, in the e-medicinal services focus the endless measure of individual information will be gone into the internet and totally lose control over their information.

In past two years nearly 8 million patients' personal data had leaked as per the survey of the government website. There are huge advantages for securing the medical data and by limiting the access. Numerous insurance agencies will also decline to give disaster protection in the wake of knowing the patients infection history. As the privacy issues are not addressed properly in previous studies, the high efforts are produced to secure the personal health data, because securing the data which is stored in cyber space is very difficult. In this way, there is a dire requirement for the improvement of reasonable conventions, designs, and frameworks guaranteeing protection and security to shield delicate and individual computerized data. Information stockpiling and computational errands turns into a prominent in the distributed computing period.

The company's claim management solutions are provided by Total Claims Capture and Control (TC3) for health care buyers such as drug sellers, insurance companies, and for Medicare payers. The sensitive health information is stored in Amazon's Elastic Compute Cloud (EC2) which has been using by TC3 to process the data which is sent by their clients. Outsourcing the calculation to the cloud helps TC3 from purchasing and looking after servers, and permits TC3 to exploit Amazon's skill to handle and investigate information speedier and more effectively. Power, convenience, flexibility, and cost efficiency of the cloud-based data/computation outsourcing paradigm had inspired the proposed cloud-assisted mobile health networking.

In proposed work the private cloud is presented which can be considered as an administration offered to versatile clients. The proposed arrangements are based on the administration model appeared. By utilizing the foundation of people in general cloud suppliers (e.g., Amazon, Google) Software as a Service (SaaS) supplier gives private cloud administrations. Portable clients outsource information preparing errands to the private cloud which stores the handled results on people in general cloud. The security and serious calculation stockpiling can be put away in the cloud.

Literature Review

A novel frame work for access controls to PHR's had proposed within cloud computing environment. Attribute Based Encryption (ABE) systems are utilized to scramble every patient's PHR information. To lessen the key dispersion multifaceted nature, the framework is separated into numerous security spaces [1]. A few inadequacies of current e-health arrangements and models are brought up, especially they don't address the customer stage security, which is a vital viewpoint for the general security of e-health frameworks[2].

Personal Health Record (PHR) are utilized as a contextual investigation, they initially demonstrated the need of hunt capacity approval that diminishes the security introduction coming about because of the indexed lists, and set up a versatile structure for Authorized Private Keyword Search (APKS) over encoded cloud information. At that point they proposed two novel answers for APKS taking into account a late cryptographic primitive, Hierarchical Predicate Encryption (HPE) [3]. A period of huge information has entered – information sets that are described by high volume, speed, assortment, exhaustivity, determination and indexicality, relationality and adaptability. Much of these data are spatially and temporarily referenced and offer numerous potential outcomes for upgrading land understanding, including for post-positivist researchers. Failing to do so could be quite costly as the discipline gets left behind as others leverage insights from the growing data deluge.[4].

DaaS (Data as a Service) methodology was proposed for wise sharing and preparing of substantial information accumulations with the point of abstracting the information area (by making it significant to the requirements of sharing and getting to) and to completely decouple the information and its handling. They exemplified the approach from large data collections from health and biology domains.[5].Designed an electronic medical record system with the goal that they can trade all their put away information as per open principles. Patients were offered consents to see their record and additionally creation, gathering, explanation, adjustment, dispersal, use and ensure of the record is critical to guaranteeing patients entrance to their own particular therapeutic data while securing their protection[6].

Akl and Taylor [7] and later Sadhu [8] proposed developments taking into account one-way works which are fundamentally the same to what they portrayed in the paper. All the more as of late, Hengartner and Steenkiste proposed a plan for encryption-construct access control situated in light of various leveled IBE [9]. This paper addresses this testing open issue by, on one hand, characterizing and authorizing access strategies in view of information qualities, and, then again, permitting the information proprietor to assign the majority of the calculation errands included in fine-grained information access control to untrusted cloud servers without unveiling the basic information substance. They accomplished this objective by misusing and exceptionally consolidating procedures of Attribute-Based Encryption (ABE), intermediary re-encryption, and languid re-encryption [10]. Proposed encryption plan where each approved client in the framework has his own particular keys to scramble and unscramble information. The plan underpins catchphrase look which empowers the server to return just the encoded information that fulfills a scrambled question without unscrambling it. And they gave two developments of the plan giving formal verifications of their security furthermore provided details regarding the aftereffects of a model execution [11].

Architecture Design

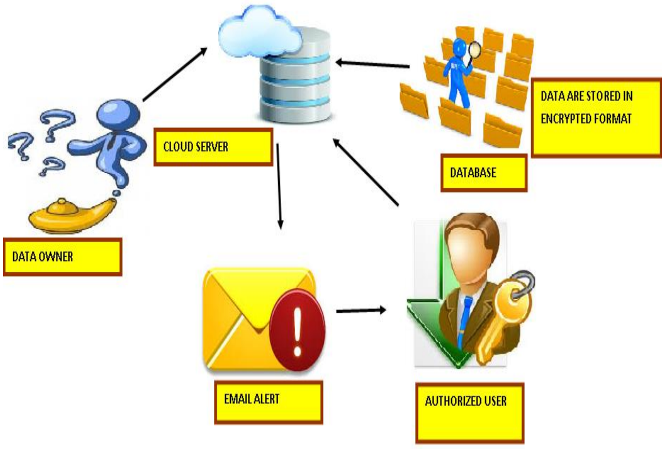


Fig 1: Architecture diagram

The architecture of the proposed method consists of five blocks as Data owner, Cloud server, Data Base, Email alert, Authorized user where each block performs its own function as Data owner who possess the medical record, data reader as who can read the encrypted medical record from the Cloud Server. Cloud Server used keyword policy attributed based encryption and generates OTP (One Time Password) through Email Alert for their Authorized users, so that the Authorized users can access the patient’s data. In the Data Base all the information of the patient is stored in Encrypted format .

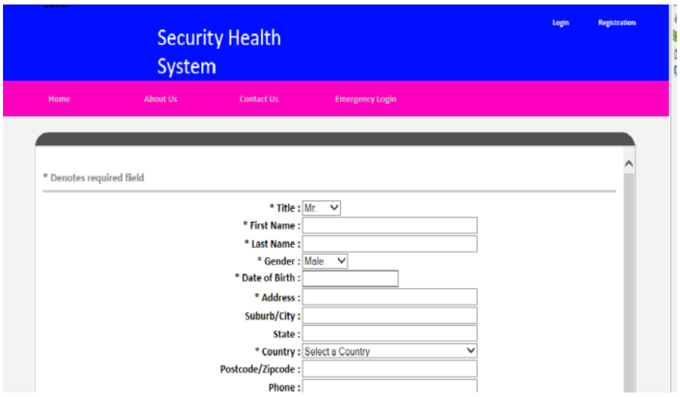
Proposed Work

A novel patient-centric framework and a suite of mechanisms for data access control to PHR are stored in semi-trusted servers. The leverage of Attribute Based Encryption (ABE) techniques to encrypt each patient’s PHR file. This system allows dynamic modification process for accessing policies or file attributes by using android application. The system design is done by using below mentioned modules.

RESULTS AND DISCUSSIONS

User Registration

Fig. 2 shows the process of user registration and providing the information of user .The patient can access the data from the server by giving their own log-in details. Without having an account they aren't able to access the files and view their medical details. So first the patient will create an account with the server by providing the necessary information like username, password, DOB, address and phone number, medicines they are using and type of diagnosis and treatment that they are taking . Once this information is provided by the user, server will store the details into the database.



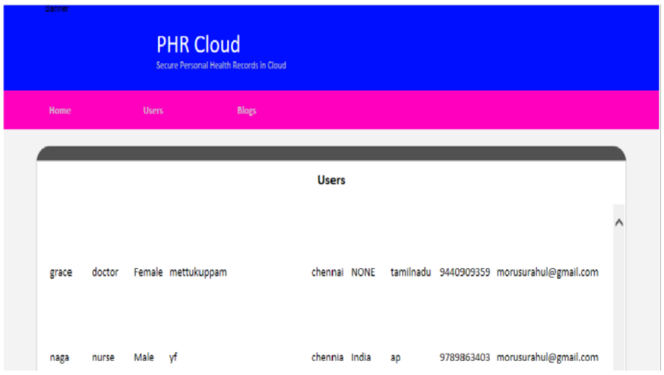
* Denotes required field

* Title : Mr.
* First Name :
* Last Name :
* Gender : Male
* Date of Birth :
* Address :
Suburb/City :
State :
* Country : Select a Country
Postcode/Zipcode :
Phone :

Fig 2: Registration of user

Cloud Ser

Cloud computing means sharing of resource. The resource will be stored in the remote server called as cloud server. In proposed system all the patient's information will be stored in the cloud servers as shown in fig.3. So that the patients information can be retrieved from the cloud server. Also the cloud server will store all the patients' information in their database for future purpose. Also they will have all the type of data regarding the personal health care.



Users

grace	doctor	Female	mettukuppam	chennai	NONE	tamilnadu	9440909359	morusurahul@gmail.com
naga	nurse	Male	yf	chennia	India	ap	9789863403	morusurahul@gmail.com

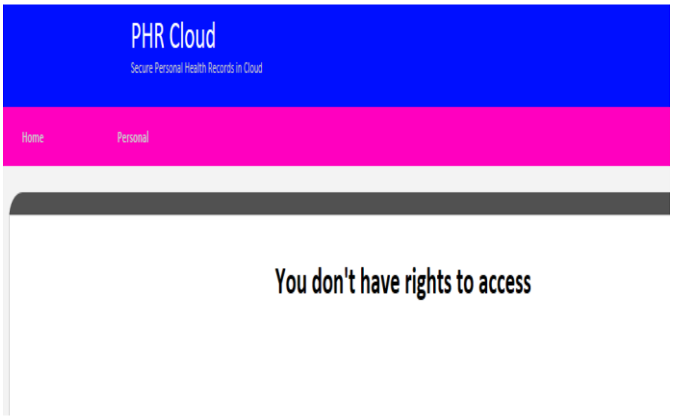
Fig 3: Storage of users data

Encryption and Decryption

In this project ABE algorithm is used to secure the data from the other user by using ABE algorithm this algorithm is type of encryption that is used to secure the data in field vice. In the proposed model ABE is used to produce the result based on the designation of the staff, if the staff overcomes their privileges, then the intimation will be given to the user.

Access Privileges

Although the cloud computing is vast developing technology, in security point of view it need more growth. To overcome this disadvantage, need to implement two types of cloud. One is public cloud and another one is private cloud. In private the patient will set the access privileges for each and every user as their wish, each and every one cant access all the accounts as shown in fig.4. In public cloud, the cloud server will set the access privileges for each and every user based on their designation. So that legitimate users can view the data stored in the cloud only up to their privilege level. They aren't allowed to view the data beyond their privileges.

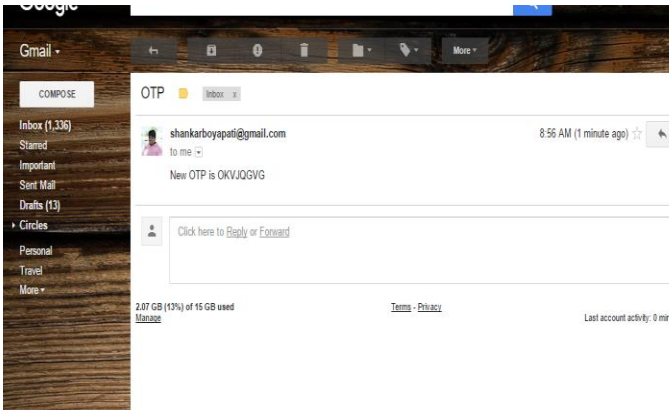


You don't have rights to access

Fig 4: Access privileges

Data View

The legitimate users are allowed to view the data cloud in the cloud server up to their privileges. To view the data stored in the cloud server, each user have to provide their authentication key then only they can able to view the data. To view the data user will get the authentication key through OTP as show in fig 5. Also the data in the cloud server will be entirely encrypted. So that it is not possible to view the data by hacking the server.



OTP

shankarboyapati@gmail.com

to me

8:56 AM (1 minute ago)

New OTP is OKVJQGVG

Click here to Reply or Forward

2.07 GB (13%) of 15 GB used
Manage

Last account activity: 0 mir

Fig 5: Generation of OTP

Emergency Conditions

When the patient's stage is critical, we can use the remote accessible technique to view the patient's records, so that we can provide the first aid to the patients. To implement this module a dynamic accessible OTP will send to the emergency department, so that with their permission, can view the patients records in the critical situation.

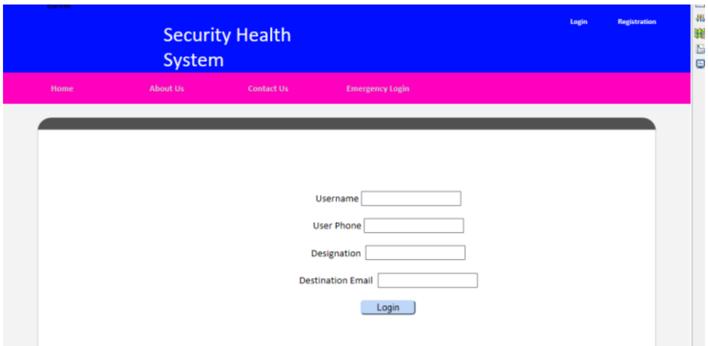
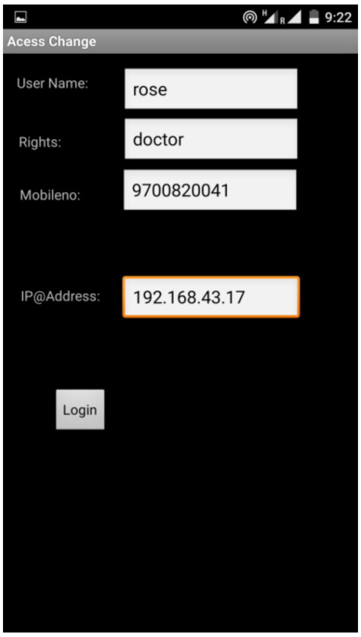


Fig 6: Emergency login

Fig.6 shows the way to login into the users account in emergency conditions, and Fig. 7 shows how the authentication will be done in Android application.



User Name: rose

Rights: doctor

Mobileno: 9700820041

IP@Address: 192.168.43.17

Fig 7: Android authentication

CONCLUSION

In proposed method secured data sharing with secured technique and OTP is generated the check integrity of the user and android access sharing is used to share the data, so this method efficiently useful for the health care system. Considering mostly dependable cloud servers, we contend that to completely understand the patient-driven concept, patients might have complete control of their own protection through scrambling their PHR documents to permit fine-grained access.

REFERENCES

[1] M. Li, S. Yu, K. Ren, W. Lou.Securing. Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010; 89–106.

[2] Sadeghi A.R, H. L¨ohr, M. Winandy. 1st ACM International Health Informatics Symposium 2010; 220–229.

[3] M. Li, S. Yu, N. Cao,W. Lou.31st International Conference on Distributed Computing Systems 2011;1-12.

[4] D. Laney.META Group Inc., 2001;File: 949.

[5] O. Terzo, P. Ruiu, E. Bucci, F. Xhafa. Seventh International Conference on Complex, Intelligent, and Software Intensive Systems 2013;475-480.

[6] B. Wixom, T. Ariyachandra, D. Douglas, M. Goul, B. Gupta, L. Iyer, U. Kulkarni, J. G. Mooney, G. Phillips-Wren,O. Turetken. Communications of the Association for Information Systems 2014; 34 (1):1-76.

[7] Selim G. Akl Peter D. Taylor. ACM Trans. Comput. Syst.,. 1983; 1(3):239–248.

[8] Ravi S. Sandhu. Cryptographic implementation of a tree hierarchy for access control. Inf. Process. Lett., .1988;27(2):95–98.

[9] Urs Hengartner and Peter Steenkiste. First International Conference on Security and Privacy for Emerging Areas in Communications Networks, Washington DC, USA, IEEE Computer Society 2005:384–396.

[10] S. Yu, C. Wang, K. Ren, W. Lou.Achieving .IEEE INFOCOM 2010; 534-542.

[11] C. Dong, G. Russello,N. Dulay.Shared.Journal of Computer Security. 2011; 19(3):367-397.