SEMANTIC AWARE SEARCHING OVER ENCRYPTED FOR CLOUD COMPUTING

INTE DIVYA [#1], **V.SARALA** [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

Abstract:

In current day's the cloud based assistance is generally received by human services suppliers so as to store and access the significant wellbeing data of patients under secure way. Consequently is essentially appeared because of the explanation like part of end clients or E-Health frameworks attempt to trade the PHRs among each other and this might be inside separation or some of the time more far separation. Henceforth we proposed a novel technique called Secure Patients Health Records for putting away the patients wellbeing data in a safe way. In this proposed application a semi-believed intermediary called Setup and Re-encryption Server (SRS) is acquainted with set up general society/private key sets and to create the re-encryption keys. Additionally, the procedure is secure against insider dangers and furthermore authorizes a forward and in reverse access control

Keywords : Re-encryption Server (SRS), proxy , E-Health, Patients Health Records

1. INTRODUCTION

The developing business of cloud has offer an assistance worldview of capacity/calculation re-appropriating assists with lessening clients' weight of IT foundation support, and decrease the expense for both the endeavors and individual clients [1], [2], [3]. In any case, because of the security worries that the cloud specialist co-op is accepted semi-trust (legit butcurious.), it turns into a basic issue to place touchy assistance into the cloud, so encryption or muddling are required before outsoucing delicate information -, for example, database framework - to cloud [4], [5], [6].The run of the mill situation for outsouced database is portrayed in Fig. 1 as that in CryptDB[7]: A cloud customer, for example, an IT undertaking, needs to re-appropriate its database to the cloud, which contains important and touchy data (for example exchange records, account data, malady data), and afterward access to the database (for example SELECT, UPDATE, and so on.) [8], [9], [10], [11], [12]. Because of the presumption that cloud supplier is straightforward yet inquisitive [13], [14], the cloud may attempt his/her best to acquire private data for his/her own advantages. Far more atrocious, the cloud could advance such delicate data to the business contenders revenue driven, which is an unsuitable working danger.

1) The security challenge of outsouced database is two-hold.
2) Sensitive information is put away in cloud, the relating private data might be presented to cloud workers;

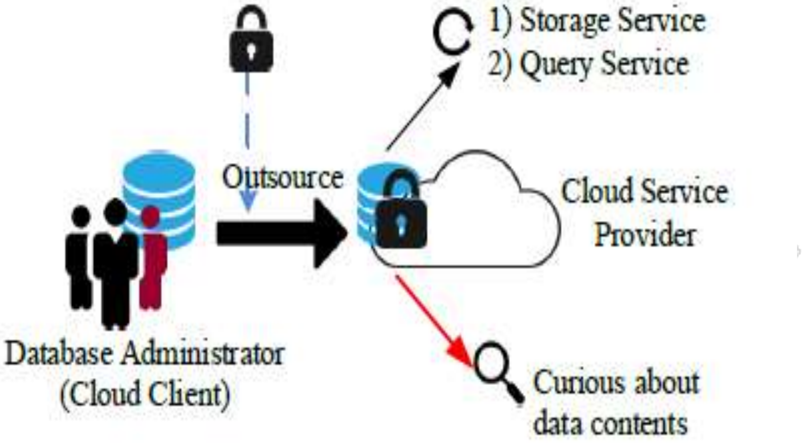


Fig. 1. Outsourced database, service and the privacy risk

2) Besides data privacy, clients' frequent queries will inevitably and gradually reveal some private information on data statistic properties. Thus, data and queries of the outsouced database should be protected against the cloud service provider

2. LITERATURE SURVEY

Writing study is the most significant advance in programming improvement process. Prior to building up the instrument, it is important to decide the time factor, economy and friends quality. When these things are fulfilled, at that point following stages are to figure out which working framework and language utilized for building up the instrument. When the software engineers begin constructing the apparatus, the developers need part of outside help. This help acquired from senior software engineers, from book or from sites. Before building the framework the above thought r considered for building up the proposed framework.

1) Public Key Encryption with Keyword Search.

Creator: D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano.

We study the issue of looking on information that is encoded utilizing an open key framework. Consider client Bob who sends email to client Alice encoded under Alice's open key. An email entryway needs to test whether the email contains the watchword "dire" with the goal that it could course the email in like manner. Alice, then again doesn't wish to enable the entryway to decode every one of her messages. We characterize and build a component that empowers Alice to give a key to the entryway that empowers the passage to test whether "earnest" is a watchword in the email without picking up whatever else about the email. We allude to this instrument as Public Key Encryption with watchword Search. As another model, consider a mail worker that stores different messages openly scrambled for Alice by others. Utilizing our instrument Alice can send the mail worker a key that will empower the worker to recognize all messages containing some particular catchphrase, however master nothing else. We characterize the idea of open key encryption with watchword search and give a few developments.

VABKS: Verifiable Attribute-Based Keyword Search Over Outsourced Encrypted Data.

Creator: Q. Zheng, S. Xu, and G. Ateniese.

It is basic these days for information proprietors to re-appropriate their information to the cloud. Since the cloud can't be completely believed, the redistributed information ought to be encoded. This anyway brings a scope of issues, for example, How should an information proprietor award search abilities to the information clients? By what means can the approved information clients search over an information proprietor's re-appropriated encoded information? By what means can the information clients be guaranteed that the cloud dependably executed the pursuit procedure for their sake? Roused by these inquiries, we propose a novel cryptographic arrangement, called unquestionable quality based catchphrase search (VABKS). The arrangement permits an information client, whose accreditations fulfill an information proprietor's entrance control strategy, to (I) search over the information proprietor's re-appropriated scrambled information, (ii) re-appropriate the monotonous inquiry tasks to the cloud, and (iii) confirm whether the cloud has dependably executed the hunt activities. We officially characterize the security necessities of VA B K S and portray a development that fulfills them. Execution assessment shows that the proposed plans are functional and deployable.

3. EXISTING SYSTEM

In the existing cloud servers, there was no concept like encryption of cloud data and also there was no facility like key generation and maintenance of data. The current cloud storage is almost centralized and all the data which is stored along with details of data owners and data users is clearly visible by the cloud server department, which is almost a big problem in the current cloud service providers. In the existing clouds there is no security for the personal health records which is generated by the hospitals and also there is no security for the reports generated by the PHR.

LIMITATION OF EXISTING SYSTEM

The following are the limitation of existing system. They are as follows:

In the existing or current clouds the following are the main limitations that are available

1. All the existing schemes are limited upto data storage and retrieval in a plain text manner.
2. All the current cloud servers don’t have a facility to store the data in an encrypted manner.
3. The existing cloud servers are almost operated in a centralized manner, where all the access can be viewed and monitored by the cloud service providers.
4. There is no concept like Setup and Re-Encryption Server (SRS) generation for the PHR records in order to provide more security for the patient centric data

4. PROPOSED SYSTEM

As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and also authorization of data for the valid users. In this paper, we proposed and analysed a secure cloud data storage of PHR records by the valid PHR Owners. Here the PHR owner can upload patient details and also assign the reports for the valid PHR users. These PHR owner and PHR user need to get access key from the cloud server and once if the cloud grants key privileges then only user can access the files and corresponding reports in a secure manner.

ADVANTAGES OF THE PROPOSED SYSTEM

The following are the advantages of the proposed system. They are as follows:

1. Our protocol supports multi access which provides a great flexibility for the system to set different access policies for individual users according to different scenarios.
2. At the same time, the privacy of the user is also preserved. The cloud system only knows that the user possesses some required attribute, but not the real identity of the user.

3. To show the practicality of our system, we simulate the prototype of the protocol.We finally show that our proposed approach is best in giving security for the PHR records which is ploaded by the medical persons

5. MODULES

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. We have implemented the proposed concept on Java programming language with JEE as the chosen language in order to show the performance this proposed novel IPath protocol. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My-SQL Server. The application is divided mainly into following 3 modules. They are as follows:

1. Cloud Module
2. Setup and Re-encryption Server Module
3. User Module

Now let us discuss about each and every module in detail as follows:

5.1 Cloud Module

The scheme proposes the storage of the PHRs on the cloud by the PHR owners for subsequent sharing with other users in a secure manner. The current cloud server is almost un-trusted because all the data which is stored by PHR owner can be viewed and accessed by anyone within the PHR users. So in order to avoid this problem in this current application we try to launch SRS module so that the data from the cloud server can be accessed only by the valid users who got secret key from SRS and those users only can access the file in a plain text manner. Remaining all users can’t able to access the file in a plain text manner.

5.2 Setup and Re-encryption Server Module

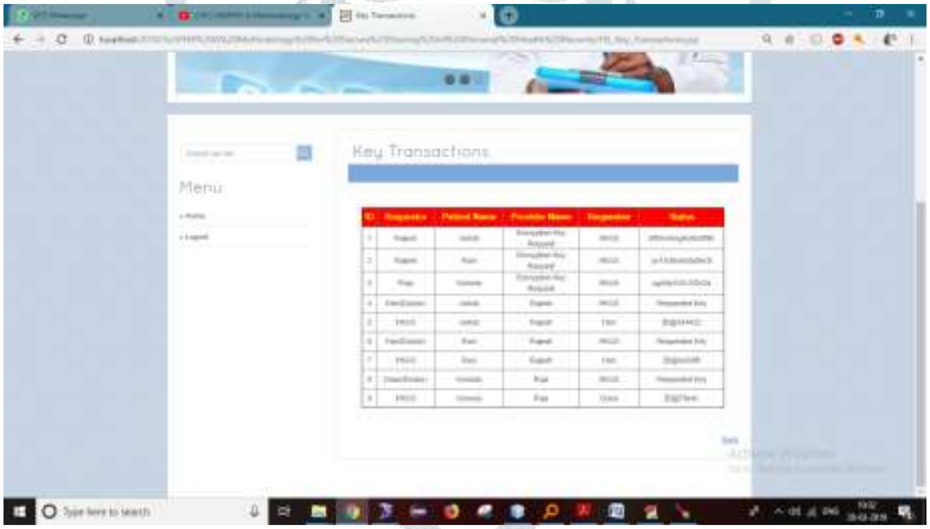
In this application the SRS is a module which is newly integrated for the current cloud server in order to generate public and secret key for the PHR files.All the data owners who try to upload the PHR files try to send a list for the end users in terms of Filenames and File Secret keys.The filenames are viewed by every one hence it is public in nature but the secret keys are given only for the authorized users.The SRS takes the total responsibility in generating the secret key for the requested users and in turn send those keys for downloading the data in a plain text manner.This generation process is known as Re-Encryption Server where the data user will receive a key for accessing the file in a plain text manner.

5.3 Data User Module

Here there are two types of users present in the application: One type of user is PHR data owner and other type is PHR data user.The PHR data owner is one who try to encrypt the files and upload all the files into the cloud server and he also sends a copy of encrypted parameters to the SRS server in order to maintain a index for all the encrypted files.Now the PHR data user is one who try to register and login into his account for requesting the PHR records from the cloud server.So the user try to request different PHR files ,in which some are related and some are not related to that appropraite user.Here the SRS server try to identify the user details before granting the permissions and once if the SRS allow the user for accessing the file he will send a secret key for accessing the file in a plain text manner.Those users who don't have that access permission will always see the data in a encrypted manner

6. RESULTS AND SCREENS

User Transactions



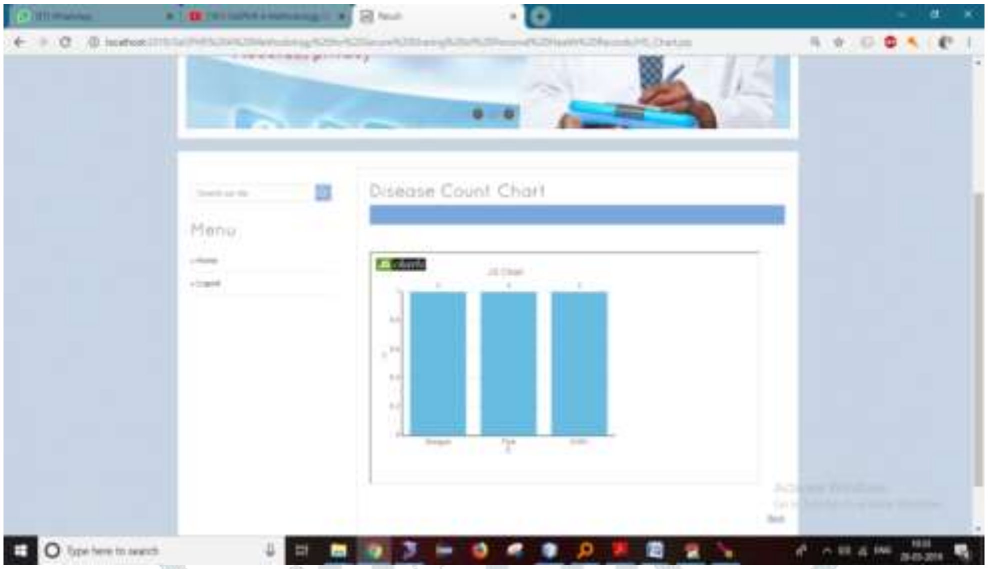
Key Transactions

Menu

ID	Requestor	Patient Name	Provider Name	Requestee	Status
1	[illegible]	[illegible]	Encryption Key Request	[illegible]	[illegible]
2	[illegible]	[illegible]	Encryption Key Request	[illegible]	[illegible]
3	[illegible]	[illegible]	Encryption Key Request	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]	[illegible]	Requested Key
5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
6	[illegible]	[illegible]	[illegible]	[illegible]	Requested Key
7	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
8	[illegible]	[illegible]	[illegible]	[illegible]	Requested Key
9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Figure Represents the Key Transactions of All Registered users

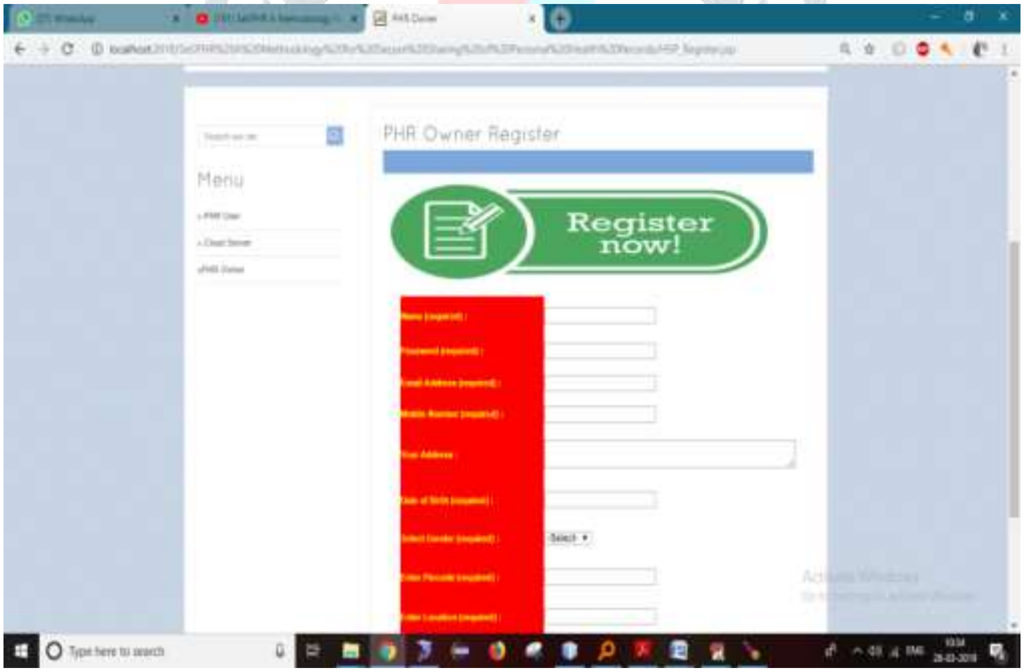
View Result in Chart Manner



Disease Count Chart

Figure Represents the Result in chart Manner

PHR Owner Registration Module



PHR Owner Register

Name (required) :

Password (required) :

Email Address (required) :

Mobile Number (required) :

Your Address :

Date of Birth (required) :

Select Gender (required) : Select ▾

Enter Pincode (required) :

Enter Location (required) :

Figure . Represents the PHR Owner Registration Module

7. CONCLUSION

We proposed a procedure to safely store and transmission of the PHRs to the approved substances in the cloud. The system saves the privacy of the PHRs and authorizes a patient-driven access control to various parts of the PHRs dependent on the entrance favorable to vided by the patients. We executed a fine-grained get to control technique so that even the legitimate framework clients can't get to those bits of the PHR for which they are not approved. The PHR proprietors store the scrambled information on the cloud and just the approved us-ers having substantial re-encryption keys gave by a semi-believed intermediary can unscramble the PHRs.

8. REFERENCES

1) M. Armbrust, A. Fox, R. Griffith, A. D. Joseph et al., “A view of cloud computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010.

2) C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward secure and dependable storage services in cloud computing,” IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

3) K. Xue and P. Hong, “A dynamic secure group sharing framework in public cloud computing,” IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

4) J.W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security. CRC press, 2016.

5) D. Zissis and D. Lekkas, “Addressing cloud computing security issues,” Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, 2012.

6) H. T. Dinh, C. Lee, D. Niyato, and P. Wang, “A survey of mobile cloud computing: architecture, applications, and approaches,” Wireless Communications and Mobile Computing, vol. 13, no. 18, pp. 1587–1611, 2013.

7) R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, “CryptDB: protecting confidentiality with encrypted query processing,” in Proceedings of the 23rd ACM Symposium on Operating Systems Principles. ACM, 2011, pp. 85–100.

8) C. Curino, E. P. Jones, R. A. Popa, N. Malviya et al., “Relational cloud: A database-as-a-service for the cloud,” 2011.

9) D. Boneh, D. Gupta, I. Mironov, and A. Sahai, “Hosting services on an untrusted cloud,” in Advances in Cryptology-EUROCRYPT 2015. Springer, 2015, pp. 404–436.

10) X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” IEEE Transactions on Computers, vol. 65, no. 10, pp. 3184–3195, 2016.

11) X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.

12) S. Benabbas, R. Gennaro, and Y. Vahlis, “Verifiable delegation of computation over large datasets,” in Annual Cryptology Conference. Springer, 2011, pp. 111–131.

13) W. Li, K. Xue, Y. Xue, and J. Hong, “TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage,” IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484–1496, 2016.

14) K. Xue, Y. Xue, J. Hong,W. Li, H. Yue, D. S.Wei, and P. Hong, “RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953–967, 2017.

15) R. A. Popa, F. H. Li, and N. Zeldovich, “An ideal-security protocol for order- on Security and Privacy (SP’13). IEEE, 2013, pp. 463–477.

16) J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, “Security and privacy-enhancing multicloud architectures,” IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 212– 224, 2013.

17) Y. Elmehdwi, B. K. Samanthula, and W. Jiang, “Secure k-nearest neighbor query over encrypted data in outsourced environments,” in 2014 IEEE 30th International Conference on Data Engineering. IEEE, 2014, pp. 664–675.