International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume – 3, ISSUE – 4 **ISSN (Online):2454- 1966**

Research Manuscript Title

SECURITY SHARING OF PHR IN CLOUD STORAGE USING CIPHER TEXT POLICY

D.Radhika[1], G.Priyanka[2]

[1]Assistant Professor, Vivekanandha College of Engineering for Women, Namakkal

[2]PG Student, Vivekanandha College of Engineering for Women, Namakkal

E-Mail-ID:priyankariya1094@gmail.com

December – 2017

www.istpublications.com

International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume – 3, ISSUE – 4 ISSN (Online):2454- 1966

SECURITY SHARING OF PHR IN CLOUD STORAGE USING CIPHER TEXT POLICY

D.Radhika[1], G.Priyanka[2]

[1]Assistant Professor, Vivekanandha College of Engineering for Women, Namakkal

[2]PG Student, Vivekanandha College of Engineering for Women, Namakkal

E-Mail-ID:priyankariya1094@gmail.com

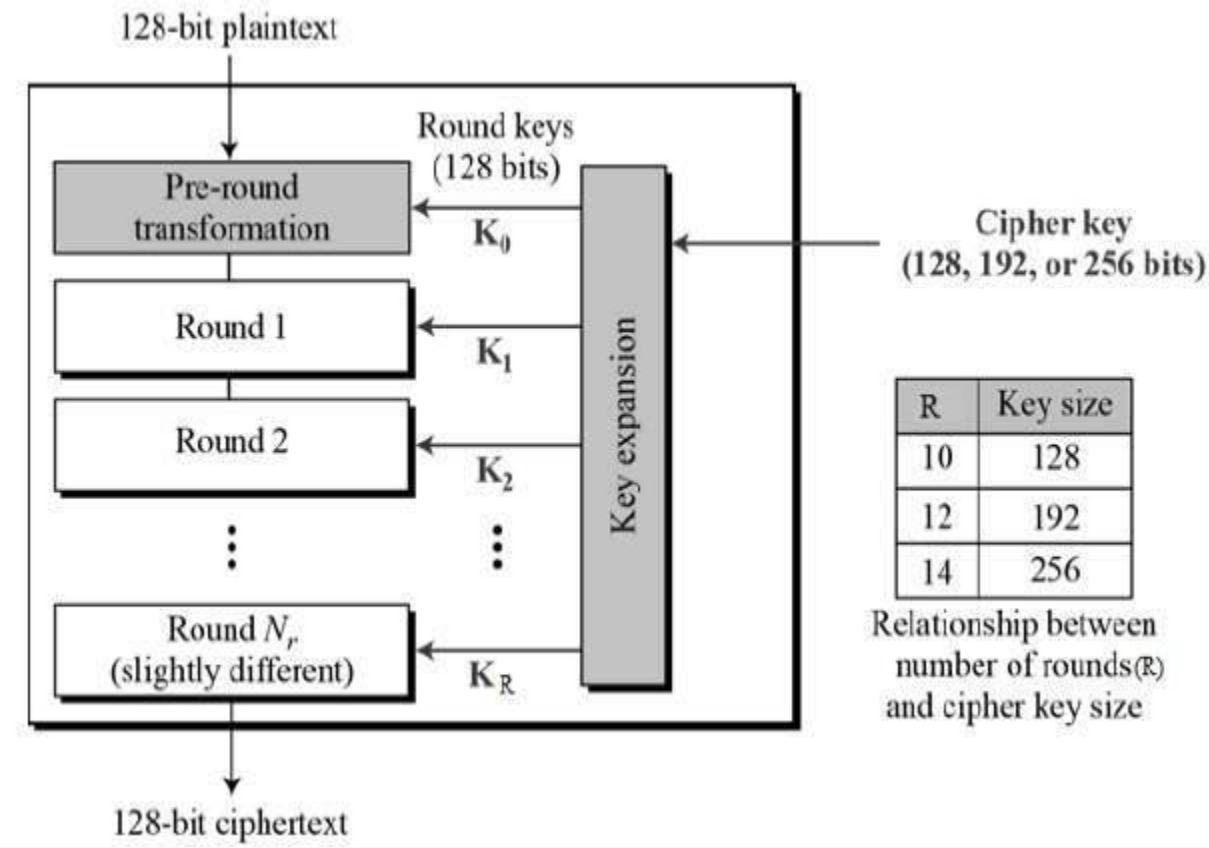
ABSTRACT

Personal Health Records or PHR is the medical information of an individual, stored and managed by the patient himself, in third party servers like clouds, so as to make it available for global data sharing. As the usage of such servers for storage purposes become more complex, they give rise to various security issues. Privacy, scalability and flexibility are some common issues concerning third party servers. There are different types of approaches are used to protect the privacy of the system. In this paper, some encryption techniques such as attribute based encryption (ABE), Cipher text policy-Attribute based encryption (CP-ABE), Multi-Authority Attribute based encryption (MA-ABE) and key policy Attribute based encryption (KP-ABE) are discussed. A high degree of patient privacy is guaranteed simultaneously exploiting multi authority ABE. This scheme also enables dynamic modification of access policies or file attributes, support efficient on demand user/attribute revocation. This scheme also supports efficient on-demand user revocation. We have proven its efficiency by implementation.

Key Terms: *Flexibility, Access Policy, Scalability, Attribute Based Encryption (ABE).*

1. INTRODUCTION

PHR is also a tool for global medical data sharing. Thus an authorized medical care provider can have access to a patient's health related information and thereby gains more insight into the health history of the patient under his care. Cloud Computing, one of the most powerful paradigms in the IT sector, is a way to increase capacity on the fly without investing in new infrastructure, training new personnel, or licensing new software. However cloud computing means storage of data on the internet. The outsourcing of PHR data on to clouds has led to concerns of the insecurity of the medical information. The medical information of an individual is highly sensitive and must be accessed only by the patient or by those who has been given authorization by the patient. The data must remain confidential to all else.



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

This system is given that the fine grained access to the system by using the different attributes based encryption techniques. This user of the system are classified into two security of the domains such as personal domain (PSD),which includes family members and friends, and public domain (PUD) , which includes medical researchers , doctors, health care organization, nurses, and insurance field. Most health care providers and different vendors related to healthcare information technology started their PHR services as a simple storage service. Then turn them into complicated social networks like service for patient to sharing health information to others with the emergence of cloud computing.

2. LITERATURE REVIEW

While reviewing a scheme we listed the algorithms and techniques used in that scheme and the merit and demerit of that scheme are also specified. The following papers are survived in this section

In [1] authors Ming Li, Shucheng Yu, Ning Cao Wenjing Lou **"Authorized Private Keyword Search over Encrypted Data in Cloud Computing"** describe about the Personal Health Record (PHR) as a case study, we first show the necessity of search capability authorization that reduces the privacy exposure resulting from the search results, and establish a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data. The data may very sensitive information, such Personal Health Records (PHR), facebook photos, and business documents. Many people remain about the levels of privacy protection of their data when stored in a server owned by a third-party cloud service provider. PKC based schemes not have problem, but if every user obtains restricted search capabilities from a central trusted authority (TA) who assumes the responsibility of authorization at the same time, it shall be

always online, dealing with large workload, and facing the threat of single-point-of-failure. Merit of the system category is they obviate the overhead for users to acquire search capabilities. Demerits of system reduce the maintenance cost.

In [2] authors Feras Aljumah, Makan Pourzandi, Mourad Debbabi **"Privacy-Preserving Querying Mechanism on Privately Encrypted Personal Health Record**s**"** describe about privacy of the data remains a concern due to the sensitive nature of the data. Such systems include cloud-based personal health record (PHR) or financial management systems. In the market today, there are many solutions which have been presented to provide users with cryptographically secure storage. PHR systems are patient centric systems that allow patients to store and manage health data stored on the cloud. Many of the current PHR system providers have the ability to access all patient records. Even though PHRs might be encrypted in the cloud, the keys are being managed by the same provider. As such, it is possible for intruders with access to the cloud provider's infrastructure to gain access to all the records. Merit of the system protocol relies on semantically secure probabilistic cryptosystems. Demerit of system protocol that allows third parties to execute various types of queries on privately encrypted data stored in an untrusted cloud while preserving the privacy of both.

In [3] authors Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk **"A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing"** propose scheme only to efficiently share their private health data among a variety of users including healthcare professionals as well as family and friends. PHRs are usually outsourced and stored in third-party cloud platforms which relieves PHR owners from the burden of managing their PHR data while achieving better availability of health data. Ensure PHR owners' control of their outsourced PHR data, attribute based encryption (ABE) mechanisms have been considered. considering the fact that cloud infrastructures are managed by third-parties who may be curious about the data being stored, privacy concerns have been raised on the stored data [3] [4]. Also such storage servers could become targets for various malicious activities and may lead to illegal exposure of sensitive data belonging to patients. Merit of the system is PHRs is the fact that the private health data is always under the control of the patient unlike EHRs since they are under the control of individual care deliverers. Demerit of system ABE driven PHR sharing schemes is that PHR data are encrypted with a pre-decided attribute based access structure.

In [4] authors Kai Fan, Nana Huang Yue Wang Hui Li Yintang Yang **"Secure and Efficient Personal Health Record Scheme Using Attribute-Based Encryption"** determine about the emergence of cloud computing, personal health record (PHR), which is envisioned to exchange health information has attracted much attention of researchers. The PHR service allows each patient to have a complete control of her medical history. we mainly adopt attribute-based encryption (ABE) as the primitive encryption in the public domain, which enables the patient to
set an access policy to encrypt his PHR, and only the users whose own attributes satisfied the access policy can decrypt it. the ciphertext length grows linearly with the number of users. there are multiple domains, multiple owners, multiple AAs, and multiple users. In addition, for each PSD the Key-Aggregate Encryption called KAE is exploited to implement the read access permission; for each PUD, our proposed revocable MA-ABE based on outsourcing decryption scheme is used. Merit of the system supports a tree access structure. But demerit of capacity want to divide control of the various attribute over many different authorities.

In [5] authors Shruthi Suresh **"Highly Secured Cloud Based Personal Health Record Model"** it determines a Personal Health Records are also outsourced to cloud and hence security is a major issue. Privacy and fine grained data access control are other risks in securing health records. Attribute Based

Encryption is a variant of asymmetric encryption in which the secret key of the user and the cipher text depends upon attributes used. In such a system, the decryption of a cipher text is possible only if the set of attribute of the user key matches the attribute of the cipher text. ABE not only offers fine grained access control but also prevents against collusion. It reduced the high key management overhead and requires encrypting multiple copies of a file using different user's keys. Using ABE, access policies expressed based on the attributes of the user data which enable the patient to selectively share the PHR among a set of users by encrypting the file under a set of attributes, and so the owner don't want to know the complete list of users. The main goal for this technique is to provide security, access control and the main aspects are to provide flexibility, scalability, and fine grained access control. Merit of the system scalable, flexible and highly secure cloud based health record system is described.
Demerit of system the data owner is also a trusted authority (TA) . KPABE that the encrypted data cannot choose who can decrypt it.

In [6] authors Neetha Xavier, V.Chandrasekar **" Security of PHR in Cloud Computing by Using Several Attribute Based Encryption Techniques"** it describe a Personal Health Record (PHR) has developed as the emerging trend in the health care technology and by which the patients are efficiently able to create, manage and share their personal health information. This PHR is now a day's stored in the clouds for the cost reduction purpose and for the easy sharing and access mechanism. The main concern about this PHR is that whether the patient is able to control their data or not. It is very essential to have the fine grained access control over the data with the semi-trusted server. Electronic health record is the electronic version of the medical record of the care and treatment the patient receives. It is maintained and managed by the health care organizations.
The data owner is uploading the data to the cloud server after encrypting the data according to the access control policy defined with the set of attributes. Merit of the system The PHR will use more secure encryption primitives in the future. Demerit of key management problems and complexity.

In [7] authors Luan Ibraimi, Muhammad Asim, Milan Petko vic**"Secure Management of Personal Health Records by Applying Attribute-Based Encryption"** it propose a Traditional access control mechanisms have several limitations with respect to enforcing access control policies and ensuring data confidentiality. In particular, the data has to be stored on a central server locked by the access control mechanism, and the data owner loses control on the data from the moment when the data is sent to server. industry and a number of standards under development to provide the interoperability across different PHR and EHR services, confidentiality of patient's health information remains a major obstacle with respect to the adoption of the PHRs by the individuals. Our scheme allows a patient to store her PHRs in an encrypted form on a commercial PHR system and share them securely with other users who belong to two different security domains: (a) professional domain (PD) - a group of healthcare providers e.g. doctors, nurses, or (b) social domain (SD) - her family, friends, or fellow patients. Merit of system secure management of personal health records. Demerit of system un-trusted web server.

In [8] authors Suhair Alshehri, Stanisław P. Radziszowski, and Rajendra K. Raj **"Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption"** it describe the cloud-based data sharing platforms, privacy and security requirements can prevent their adoption in diverse domains, most notably in healthcare . The Health Information Technology for Economic and Clinical Health Act provides federal incentives to U.S. healthcare providers to encourage the meaningful adoption and use of electronic health record (EHR) systems to improve healthcare quality. CP-ABE supports complex policies to specify which secret keys can decrypt which ciphertexts: each healthcare provider's secret key is labeled with a set of attributes, and ciphertexts are associated with access policies. The security of ECC is based on the hardness of the elliptic curve discrete logarithm problem, and achieves RSA-equivalent security with a much smaller group; for example, a 163- bit key in ECC is

considered to be as secure as 1024- bit key in RSA. Merit of system A proof-of-concept cloud-based EHR is
being implemented and will be used to verify the feasibility. Demerit of system cost-effective and its components carefully implemented.

In [9] authors Raseena M Harikrishnan G R **"Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption"** it propose a patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. This scheme also enables dynamic modification of access policies or file attributes, support efficient on demand user/attribute revocation. However some practical limitations are in building PHR system. There is concern about security issues when outsource these data to the cloud server. Surveys shows that seventy five percentage people are not choose PHR system because they are concern about the security issues. For secure storing better method for designing PHR system is based on encryption method. Before outsourcing data to the third party different encryption methods are used. Merit of system is scheme is both scalable and efficient. Demerits of system Data security is the major problem in cloud storage. In practical case some more problems will arise.

In [10] authors Perumal B Pallikonda Rajasekaran M Duraiyarasan S **"An Efficient Hierarchical Attribute Set Based Encryption Scheme with Revocation for Outsourcing Personal Health Records in Cloud Computing"** it determine a It is attractive for the Personal Health Record (PHR) service providers to shift their PHR applications and storage into the cloud. Under encryption, it is excited to achieve fine grained access control to PHR data in a scalable and efficient way. It also includes the problem of establishing access control for the encrypted data, and revoking or withdrawing the access rights from users when they are no longer authorized to access the encrypted data on cloud servers. In an emergency you can quickly give vital information, such as a disease you're being treated for, drug allergies if any, medications you take, and contacted your family doctor and so on. Apart from this it also empowers you to manage your health between visits. Building and maintaining specialized data centres to outsource the PHR data makes some complexity in terms of sharing those health data with a wide range of users, including family members or friends and with healthcare providers. Third-party service providers welcome to outsource the sensitive PHR data. Merit of system better access control with most efficient and flexible. Demerit of most computational overheads. Less overhead on other.

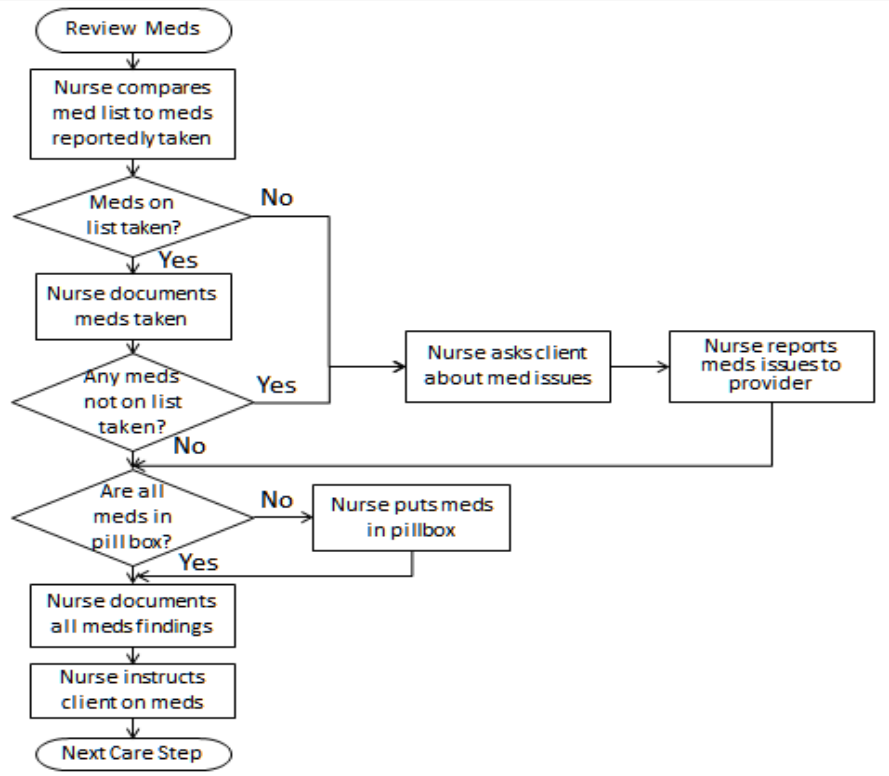
3. PROBLEM STATEMENTS

A solution to this dilemma is to encrypt the information before uploading for storage in clouds. There has been various techniques proposed for the encryption of data outsourced to clouds. One method is the usage of passwords provided by the owner/patient whenever access to a PHR file is needed. Another mechanism is the presence of a Central Trusted Authority. But all these techniques have limitations. The usage of passwords requires a PHR owner/patient to be continuously online, which is not feasible. Central Authority can lead to a single point of failure. A better suggestion, which has also been effectively implemented, is the Attribute Based Encryption (ABE) scheme. Users of the PHR service are given access to a PHR file only if they have been authorized by the PHR owner/patient, i.e., the patient. A patient's PHR file can be accessed by his relatives, friends, doctors, nurses etc. If the owner/patient is responsible for managing all details of each user key, then, keeping in mind the large and unlimited number of possible professional users, there could be heavy key management overhead.

4. PROPOSED SYSTEM

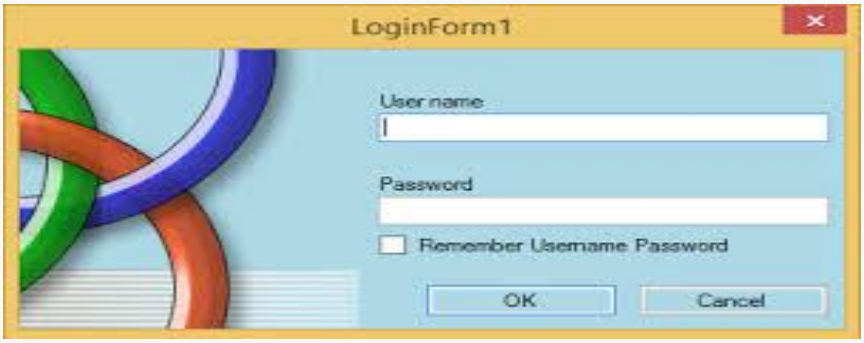
The preceding two chapters have discussed the parameterization of queueing network models of existing systems and evolving systems. Inthis chapter we consider models of proposed systems: major new systems and subsystems that are undergoing design and implementation. The process of design and implementation involves continual tradeoffs between cost and performance. Quantifying the performance implications of various alternatives is central to this process. It also is extremely challenging. In the case of existing systems, measurement data is available. In the case of evolving systems, contemplated modifications often are straightforward (e.g., a new CPU within a product line), and limited experimentation may be possible in validating a baseline model. In the case of proposed systems, these advantages do not exist. For this reason, it is tempting to rely on seat-of-the-pants performance projections, which all too often prove to be significantly in error. The consequences can be serious, for performance, like reliability, is best designed in, rather than added on. Recently, progress has been made in evolving a general framework for projecting the performance of proposed systems. There has been a confluence of ideas from software engineering and performance evaluation, with queueing network models playing a central role. The purpose of this chapter is to present the elements of this framework.

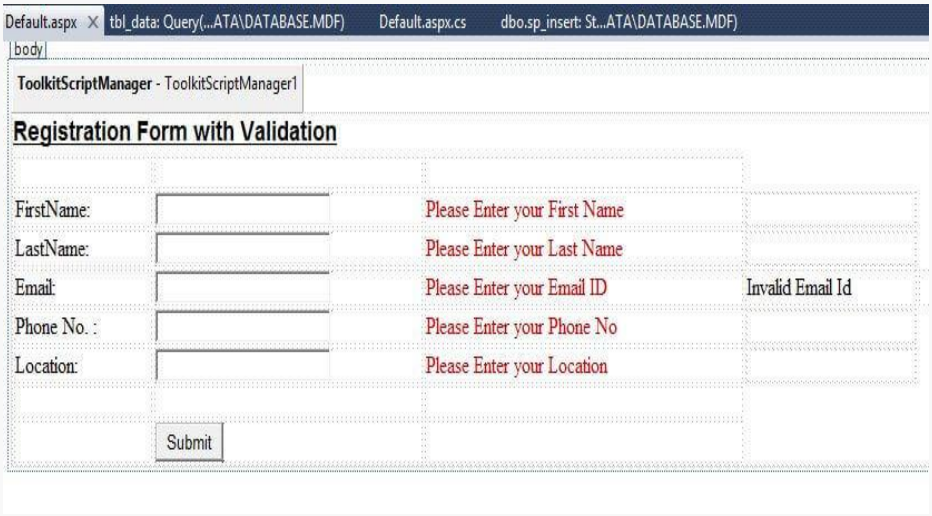
The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users' data access requirements. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector.

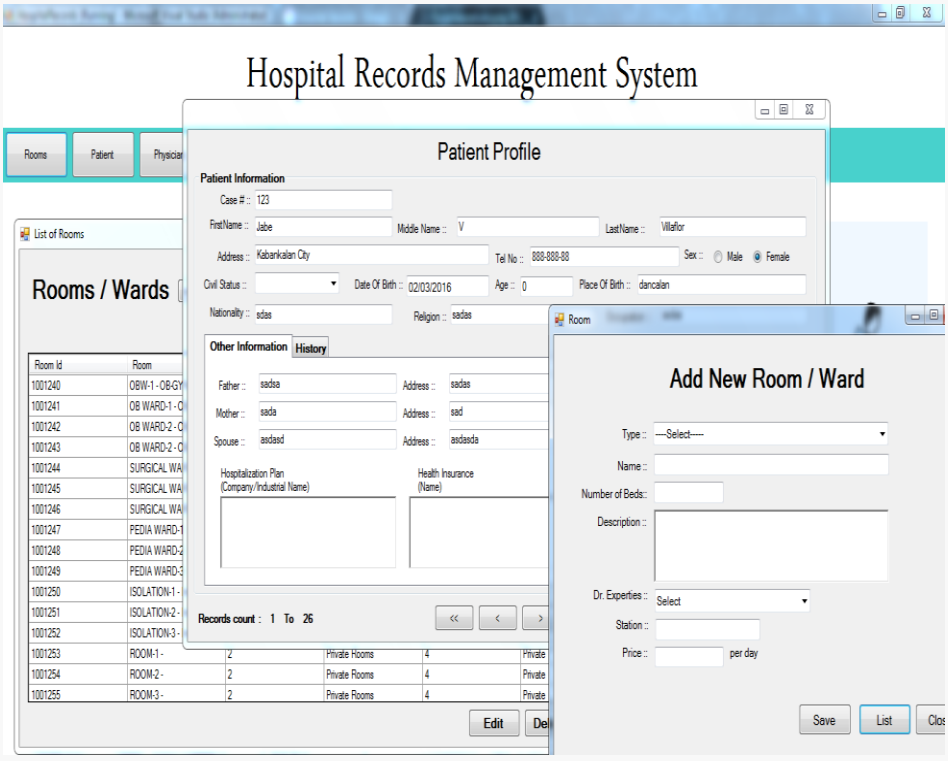


5. OUTPUT

We have seen in considering the speech-circuit that both terms involved in the linguistic sign are psychological and are united in the brain by an associative bond. This point must be emphasized. The linguistic sign unites, not a thing and a name, but a concept and a sound-image. The latter is not the material sound, a purely physical thing, but the psychological imprint of the sound, the impression that it makes on our senses. The sound-image is sensory, and if I happen to call it 'material', It is only in that sense, and by way of opposing it to the other term of the association, the concept.


LoginForm1
User name
Password
Remember Usernamе Password
OK
Cancel


Default.aspx
tbl_data: Query(...ATA\DATABASE.MDF)
Default.aspx.cs
dbo.sp_insert: St...ATA\DATABASE.MDF)
body
ToolkitScriptManager - ToolkitScriptManager1
Registration Form with Validation
FirstName:
Please Enter your First Name
LastName:
Please Enter your Last Name
Email:
Please Enter your Email ID
Invalid Email Id
Phone No. :
Please Enter your Phone No
Location:
Please Enter your Location
Submit


Hospital Records Management System
Rooms
Patient
Patient Profile
Patient Information
Rooms / Wards
Other Information
History
Add New Room / Ward
Edit
Save
List

6. PERFORMANCE ANALYSIS

During the last decade, automatic or semautomatic performance tuning of applications running on parallel systems has become one of the highly focused research areas.Performance tuning means to speed up the execution performa nce of an application. Performance analysis plays an important role in this context, because only from performance analysis data the performance properties of the plication can be observed. A cyclic and feedback guided ethodology is often adopted for optimizing the execution performance of an application every time the execution performance of the application is analyzed and tuned and the application is then sent back for execution again in order to detect the existence of further performance problems. Thus, appropriate and detailed performance data captured during the execution of an application may effectively be used to tune the performance of an application.Performance analysis tools are based on an event model of the execution. The events can be low -level events, such as a cache miss or the graduation of a floating -point instruction, as well as high level events, such as start and end of a user function. Performance analysis tools depend on the information gathered for events during the execution.

The information can be merely the existence of an event. More detailed information can also be gathered for more sophisticated analysis of the performance. The information can either be gathered in the form of summaries or individually for each event. Performance analysis in this context means getting relevant performance information from trace data. Thus the scope of performance monitoring and analysis comprises instrumentation

7. CONCLUSION

Data security is the major problem in cloud storage. Before out-sourcing PHR into the third party server different attribute based encryption schemes are used for secure storage. ABE is used to en- crypt the PHR data, and patients can allow to access not records, then various users from public domains with different professional roles ,and affiliation, also allow to the records En-hance MA ABE scheme, better on demand revocation but In practical case some more problems will arise. The main issue in this case is trying to implement work flow based conditions. For solving these issue attribute-based broadcast encryption (ABBE). Work flow Based model is implement using ABBE and also analyse security and computation cost. for this model From analysis show that this work flow based scheme is both scalable and efficient. It gives better on demand user revocation. In future it would be interesting to consider Attribute Based Broadcast Encryption system with different types of impressibility. If consider different credential are equal then Distributed ABE scheme is needed.

REFERENCE

1. Ming Li, Shucheng Yu, Ning Cao Wenjing Lou "Authorized Private Keyword Search over Encrypted Data in Cloud Computing", 2015 31st International Conference on Distributed Computing Systems.
2. Feras Aljumah, Makan Pourzandi, Mourad Debbabi "Privacy-Preserving Querying Mechanism on Privately Encrypted Personal Health Records", 2017 IEEE International Conference on Collaboration and Internet Computing.
3. Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk "A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing", 2016 IEEE 2nd International Conference on Collaboration and Internet Computing.
4. Kai Fan, Nana Huang Yue Wang Hui Li Yintang Yang "Secure and Efficient Personal Health Record Scheme Using Attribute-Based Encryption", 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing.
5. Shruthi Suresh "Highly Secured Cloud Based Personal Health Record Model", 2015 Online International Conference on Green Engineering and Technologies (IC-GET 2015).
6. Neetha Xavier, "Security of PHR in cloud computing using ABE technique", International Journal of Communication and Computer Technologies, volume 01-No.72 issue: 07, Nov 2013,pp. 265-269.
7. L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption,"technical report, Univ. of Twente, 2009.
8. S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption," in 2012 IEEE 28th International Conference on Data Engineering Workshops, Apr. 2012, pp. 143–146.
9. Raseena M Harikrishnan G R "Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption" Volume 102 - No. 16, September 2015.
10. Perumal B Pallikonda Rajasekaran M Duraiyarasan S "An Efficient Hierarchical Attribute Set Based Encryption Scheme with Revocation for Outsourcing Personal Health Records in Cloud Computing", 2015InternationalConferenceonAdvanced Computing and Communication Systems (ICACCS -2013), Dec. 19 – 21, 2015,Coimbatore, INDIA