[IJESAT] [International Journal of Engineering Science & Advanced Technology] Volume-5, Issue-3, 345-351

PRESERVING PRIVACY FOR HEALTH RECORDS AND EFFICIENT SHARING FOR EMERGENCY CLIENTS

Under Guidance of Associate.Prof. Mr.AbdhulAhad department of CSE in Lingayas Institute Of Management And Technology

Mr.M.Ramesh ,student of M.tech,depat.of CSE in Lingayas Institute Of Management And Technology.

Abstract—

Preserving privacy for health records and Efficient sharing for emergency clients in allows patients to create, manage, control and share their health in sequence with other users as well as healthcare providers. However, there have been serious privacy concerns about outsourcing patients records in stored cloud servers, not only because data storage providers are generally not covered entities under HIPAA, but also due to an increasing number of stored data breach incidents happened in recent years.In reality, Patient records service is likely to be hosted by third-party cloud service providers in order to enhance its interoperability.

The flexible access and efficient user revocation have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. OurProposed scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency worked in that paper

Keywords: ***key management ,privacy ,health records , third parity, Patient-centric, semi-trusted servers,datamining,webmining.***

I. INTRODUCTION:

Preserving privacy for health records and Efficient sharing for emergency clients in the undergone important changes along with the emergence of the data in datamining.. In a relatively broad description, put forward by the Markleinstitution, A is a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it [KJJ+08]. We recognize that the Markle Foundation description has successfully predicted the evolving of PHR in the past ten years. Most healthcare information technology vendors and healthcare providers started their patient records services as a simple storage service, and then turn them into a complicated social-network like service for patients to share personal health information with others. Currently, interest and investment in PHRs are usually motivated by goals of ef- ficiency, increasing patient empowerment, or improving disease management. However, patients' greatest concern about PHRs, as other healthcare system, is security and privacy. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 outlined the legal protections for PHR privacy and security. But, it does not address all the issues involved, especially because HIPAA only applies 1 to covered entities including health plans, healthcare clearinghouses, and healthcare providers. Emerging cloud-based PHR service provider like Dossia, Microsoft, and Google are not covered entities. Therefore, by introducing cloud computing into PHR service, several important issues regarding PHR privacy and security need better evaluation. Potentially, PHR could protect patient privacy and security in ways that are much more secure than traditional paper-based patient records, since it can provide additional security feature such as password protecting and audit tracking. However, by outsourcing PHR into a cloud server, patients lose physical control to their own healthcare data. PHRs residing on a cloud server are subject to more malicious insider and

outsider attacks than paper-based records, which exist in only a small number of physically accessible locations. Hence, we argue extra steps must be taken to provide strong privacy assurance other than directly placing those sensitive data under the control of cloud servers. One straightforward solution is encrypting sensitive data before outsourcing it into cloud server. However, applying traditional cryptography scheme on a PHR system present a major barrier to access and share PHR. PHR system users need to deal with complicated key management problem to achieve fine-grained access control when their PHRs are encrypted using symmetric key cryptography or asymmetric key cryptography [LYRL10]. In this thesis, the fundamental goal is to propose and implement a practical design to achieve fine-grained data access control of PHR data in a semi-trusted cloud computing environments. We demonstrate PHR privacy issue can be partially solved by reducing it to the underlying cryptographic and key management problem. Relying 2 on the novel one-to-many cryptography scheme, such as attribute-based encryption (ABE), we wish to construct a PHR architecture that aims to meet the following desiderata: End-to-end Encryption. In a cloud computing paradigm, we tend to assume the physical servers of cloud-based systems to be semi-trusted comparing to centralized servers behind the firewall, in that they are subjected to more malicious inside, or outside attacks, than the later one. As a result, our approach is designed to secure PHR records from the point of origin (PHR data owner) all the way to the recipient (PHR data user) in an encrypted format. Patient-Centric. In our system, patients should have full control of their medical records and can effectively share their health data with a wide range of users. In a cryptography sense, that means patients shall generate their own decryption keys and distribute them to their authorized users. Collusion-Resistant. In our setting, PHR data can be accessed by multiple users, such as healthcare provider, health insurer, family member etc. Hence, we cannot neglect the possibility that these users may intentionally or unintentionally collude together to gain access to part of PHR data they do not have right to access separately. For that reason, in our design, the PHR data should remain confidential under such a circumstance. Revocation and Delegation. A PHR system is highly dynamic. Much like a social network, patients can terminate their relation with certain PHR data user, such as a health insurer, indefinitely. In other word, patients should always retain the right to revoke access privileges and its corresponding decryption key when they fell necessary. Nevertheless, data users may have the need 3 to grant temporally part of their access right to other parties. For example, a health insurer might only allow its accounting department to access part of customers' PHR data. As a result, we should also provide a delegation mechanism in our construction. In this research, we will focus on the design and implement of a PHR system using proper cryptographic scheme. To validate our architecture, we also evaluate the applicability and efficiency of our construction.

II. Research Work:

Several patient records systems have been proposed or implemented to enable access control on patient . We classify them into two categories according to their different access control mechanisms.

Authentication-Based PHR system :

Some PHR systems choose an attribute-based access control (ABAC) scheme or a role-based access control (RBAC) scheme to manage users' access right. This type of system usually places full trust on the cloud server where the PHRs reside in. A typical example of authentication-based PHR system is Indivo X platform [ASZ+10]. Indivo is an open-source open standard personally controlled health record (PCHR) system that enables patients to own and manage their health records. Indivo provides patients the ability to share their records with different physicians, hospitals and clinics while maintaining access control properties on the patients' health records. Access control decisions are made by the Indivo server according to institutional policies and patient specified policies.

III.Cryptography-Based Patient recordsystem :

cryptographically enforced access control scheme. This type of system usually allows patients to encrypt their PHR data and distribute corresponding decryption key to authorized user. A typical example of cryptographybased system is

iHealthEMR [ALG+]. It implements a self-protecting electronic medical records (EMRs) using attribute-based encryption. In that system, patient can encrypt each node in the XML-based EMR file with an automatic generated access policy before exporting it to cloud system. PHR users' access rights are de- fined by the attributes within their private key. However, it does not solve practical problems such as key revocation and key delegation. Nevertheless, the actual implementation is limited since the encrypted XML file contains malformed metadata and, therefore, cannot be accepted by the third party cloud service such as Google Health. In our research, we demonstrate that authentication-based system can adopt our crypto-based PHR architecture by adding proper cryptographic operation into the authentication process. Therefore, our techniques can be designed to augment a authentication-based system, providing finer-grained protections and access control without the requirement of a honest cloud server. For cryptography-based PHR system, we demonstrate that attribute-based encryption (ABE) is more suitable to achieve patient-centric and fine-grained access control. We also extend other people's work by implementing a prototype security PHR application based on ABE. To facilitate our implementation, we have built a Linux library to support key-policy attribute-based encryption (KP-ABE) scheme.

proposed using We endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-basedencryption (ABE) as the main encryption primitive.

Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

IV.INPUT DESIGN:

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

V.OBJECTIVES:

1.Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2.It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user

will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

VI.OUTPUT DESIGN:

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

We use ABE as a building block of our proposed privacy-preserving PHR system. That is because ABE not only offers fine-grained access control similar to RBAC or ABAC, but also enforces data protection against semi-trusted server. However, several important issues arise when we try to create a PHR system based on ABE. Firstly, a PHR file may be operated by multiple users who the data owner may not know. It is hard to find a proper attributes universe U which can distinctly define each user. Improper attributes universe also complicates the access structure A. Secondly, A trusted authority (TA) must be employed to protect the master key and generate private keys for the system users. Therefore, in this new scenario, there might be potential communication overhead related to key management (such as update and revocation). Thirdly, the only HBC secure encryption protocol for database, like PostgreSQL or MySQL, is client-side encryption (CSE). However, completely encrypting PHR file before submitting to the server will cripple certain features of PHR system, such as generating XML report in Indivo system. We propose a privacy-preserving PHR system model based on ABE. In order to justify our proposal, we create a Linux library (libcelia) and a toolkit (kpabe) implementing 33 primitive KP-ABE. We also build an Indivo PHA which integrates the ABE-based security scheme into Indivo system. The performance of proposed model is being evaluated in two steps: First, we measure the time consumption of ABE using our toolkit and the CP-ABE toolkit created by John Bethencourt.Then, we measure the actual data query time when data is encrypted with ABE using our Indivo PHA.

III.SYSTEM ARCHITECTURE

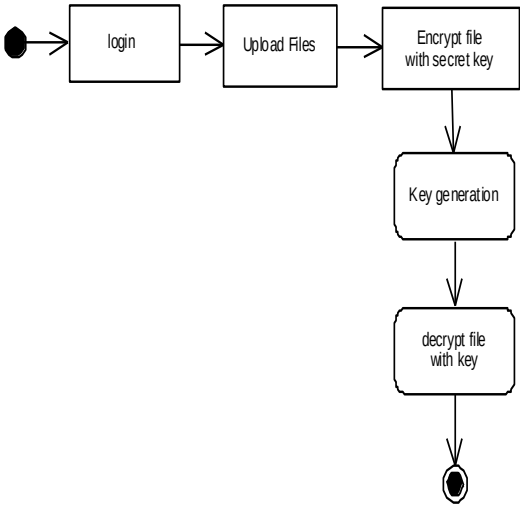


Fig:Architecture diagram of Personal Health Record User

We would like to construct a PHR system that enhances the functionality and semantic interoperability of PHR data. Therefore, we consider the fact that not only patients but also healthcare providers will participate in aggregating PHR data. The overall system architecture is similar to an advanced E-Health Cloud model [LSW10]. Figure 4.1 illustrates our system architecture and the involved parties. There are four essential parties in our architecture: patient, health care provider, trust authority, data user. A patient is the person who own PHR data. He or she should be able to collect, manage and share his or her PHR data with other data users. A health care provider is a health professional or hospital which manages patients' electronic health records (EHR). Transitionally, patients' EHR are managed locally by health care providers. In our system, health care providers can export patients' EHR into patients' PHR repositories to ease the document transfer process when patients switch health care providers. A trust authority (TA) is usually an organization expected to be responsible for supervising healthcare information exchange among healthcare system. The regional health information organization (RHIO) is a typical TA. Since our system is build upon cryptography scheme, a TA here should also be responsible for distributing decryption keys to corresponding medical personnel. A data user is the person who is allowed to view a patient's PHR file. It can be a patient's family member, a patient's friend, a health insurance company, etc. In the proposed PHR system, PHR server stores multiple copies of individual PHR file. Those copies can be encrypted under different cryptography schemes. The purpose of this setting is to preserve the veracity of the patients' PHR information. Consider the following scenario, Healthcare providers export patients medication profiles into the PHR server.

High level Functions and AES Encryption :

The Toolbox (kpabe) is a set of programs implementing the high level functions of KP-ABE scheme. There are four programs in the toolbox, which are kpabe-setup, kpabe-keygen, kpabe-enc and kpabe-dec. Each program can be used as a standard shell command. Since pairing (bilinear mapping) is quite computationally expensive, we use AES symmetric key encryption to encrypt the actual plaintext and use KPABE to encrypt the symmetric key.

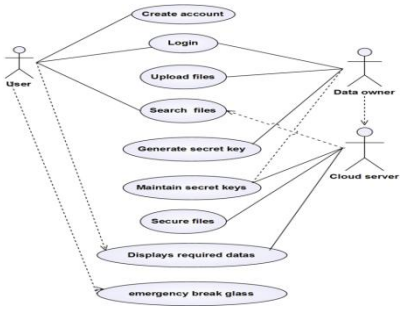


Fig:Use case diagram

VII.Patient Record System and Data mining:

There are four emerging PHR system. Based on the primary source of data for the PHR, they are de_ned as provider-tethered, payer-tethered, third-party/free standing, and interoperable PHR system. All of them can be derived from the hub and spoke model above [KJJ+08]. For example, a provider-tethered or a pay-Google AppEngine or Microsoft Azure [JASZ11, 3][Zhu10, 22].
tethered PHR system can be considered in the hub and spoke model with just one
thick spoke (provider-tethered PHR system are tied to a healthcare organizationsinternal record system; payer-tethered systems are tied to a given payers system).
A third-party/free standing PHR system can be considered in the hub and spokemodel without any spoke (consumers act as relays in third party/free standing PHRsystem to aggregate data from di_erent, unconnected sources). An interoperablePHR system can be considered as a full version of hub and spoke model.
According to the hub and spoke model, interoperability represents a key componentof PHR system. If a PHR system cannot exchange data with other healthcaresystems, PHR will become isolated from other healthcare information, with limited
access and transient value [KJJ+08]. Therefore, the minimal requirements of a PHRsystem are being capable of exporting data to and importing data from other systems
in a standardized way. More advanced PHR system in the future will function as seamlessly integrated, interoperable subsystem of other health systems [LSW10].

Linear Secret-Sharing Scheme:

The idea of linear secret-sharing scheme (LSSS) and monotone span programs was discussed by Amos Beimel [Bei96]. In a LSSS, dealer holds a secret and distributes the shares of the secret to parties. Parties can

reconstruct the secret from a linear combination of the shares of any authorized set. A famous example of LSSS is the Shamir t-out-of-n threshold scheme. In that scheme, the hardness of secret reconstruction depends on the hardness of polynomial reconstruction. We briey reiterate some of the de_nitions from Beimel's work to formally de_ne a LSSS.

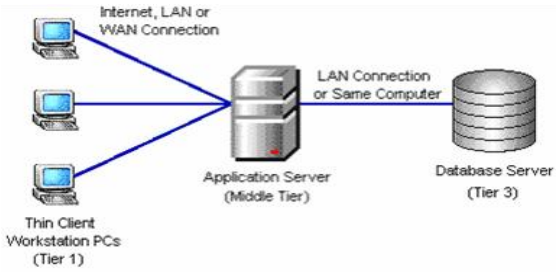
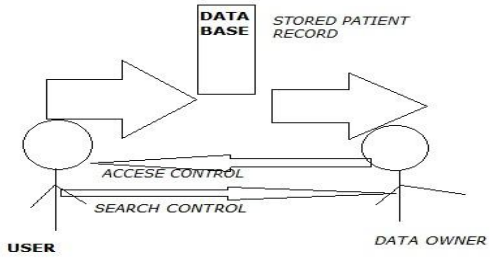


Fig:Data Flow 3-tire architecture.



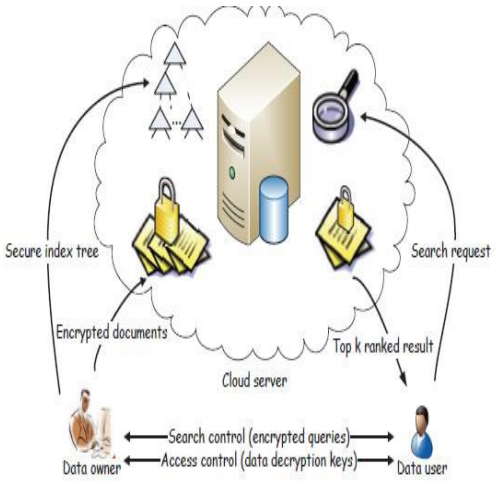


Fig:Architecture for AES

VIII. SYSTEM STUDY:

FEASIBILITY STUDY:

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY:

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on theavailable technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is

also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

IX.CONCLUSION:

we have proposed a novel framework of secure sharing of personal health records IN the data mining domain. Considering partially trustworthy data retrieval servers , we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their patient records files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Furthermore, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient and patient records to the process of the data mining process the work done.

Reference:

[1].[ALG+] J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson,and A.D. Rubin. Self-protecting electronic medical records usingattribute-based encryption. Technical report, Cryptology ePrintArchive, Report 2010/565, 2010. http://eprint. iacr. org/2010/565.

[2].[ASZ+10] B. Adida, A. Sanyal, S. Zabak, I.S. Kohane, and K.D.Mandl. Indivo x:Developing a fully substitutable personally controlled health record platform.In AMIA Annual Symposium Proceedings, volume 2010, page 6.American Medical Informatics Association, 2010.

[3] [Bei96] A. Beimel. Secure schemes for secret sharing and key distribution. DScdissertation, 1996.

[4].[BSW07] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attributebasedencryption. 2007.

[4].[GPSW06] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryptionfor _ne-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer andcommunications security, pages 89{98. ACM, 2006.

[5].[Kau09] L.M. Kaufman. Data security in the world of cloud computing. Security& Privacy, IEEE, 7(4):61{64, 2009.

[7] H. Pan, Green Data Centers monthly newsletter February 2010, Information Gatekeepers Inc.

[8] Rackspace, Cloud servers, URL: http://www.rackspace.com.

[9] IEEE Standards Association and Others, IEEE STD 1061-1998, IEEE standard for a software quality metrics methodology, 1998.

[10] W. Sobel, S. Subramanyam, A. Sucharitakul, J. Nguyen, H. Wong, S. Patil, A. Fox, D. Patterson, Cloudstone: multi-platform, multi-language benchmark and measurement tools for web 2.0, in: Proceedings of Cloud Computing and its Application, Chicago, USA, 2008.

[11]C.Harmony,Cloudharmony.com, February2012., http://cloudharmony.com/.

[12] A. Li, X. Yang, S. Kandula, M. Zhang, CloudCmp: comparing public cloud providers, in: Proceedings of the 10th Annual Conference on Internet Measurement, Melbourne, Australia, 2010.

[13] M. Zeleny, Multiple Criteria Decision Making, vol. 25, McGraw-Hill, New York, 1982.

BIOGRAPHIE:

Mareedu.Rameshpursuing M.Tech inLingayas institute of Management and Technology in the stream of Computer Science and Engineering and he received Bachelor of computer science and engineering (BTech) from Vahini Institute of Science and Technology. He born on 03.06.1991.