IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 01-05

Cloud Based Secured Health Record Storage System With Key Generation And Attribute Based Encryption

[1]P.Arun kumar,S.Santhosh kumar, A.ShahulAmeed,
UG Student, [2] Dr.A.jagan, Assistant Professor
[1](Dept Of Computer Science And Engineering, Surya Group Of Institution, Vikravandi)
[2](Dept Of Computer Science And Engineering, Surya Group Of Institution, Vikravandi)
Corresponding Author: [1]P.Arun Kumar

Abstract: *Data deduplication is a technique for eliminating duplicate copies of data, and has been widely used in cloud storage to reduce storage space and upload bandwidth. Promising as it is, an arising challenge is to perform secure deduplication in cloud storage. Although convergent encryption has been extensively adopted for secure deduplication, a critical issue of making convergent encryption practical is to efficiently and reliably manage a huge number of convergent keys. This paper makes the first attempt to formally address the problem of achieving efficient and reliable key management in secure deduplication. We first introduce a baseline approach in which each user holds an independent master key for encrypting the convergent keys and outsourcing them to the cloud. However, such a baseline key management scheme generates an enormous number of keys with the increasing number of users and requires users to dedicatedly protect the master keys. To this end, we propose Dekey, a new construction in which users do not need to manage any keys on their own but instead securely distribute the convergent key shares across multiple servers. Security analysis demonstrates that Dekey is secure in terms of the definitions specified in the proposed security model. As a proof of concept, we implement Dekey using the Ramp secret sharing scheme and demonstrate that Dekey incurs limited overhead in realistic environments.*

I. Introduction

Fast access to health data enables better healthcare service provisioning, improves quality of life, and helps saving life by assisting timely treatment in medical emergencies. Anywhere-anytime-accessible electronic healthcare systems play a vital role in our daily life. Services supported by mobile devices, such as home care and remote monitoring, enable patients to retain their living style and cause minimal interruption to their daily activities. In addition, it significantly reduces the hospital occupancy, allowing patients with higher need of in-hospital treatment to be admitted. While these e-healthcare systems are increasingly popular, a large amount of personal data for medical purpose are involved, and people start to realize that they would completely lose control over their personal information once it enters the cyberspace. According to the government website [1], around 8 million patients' health information was leaked in the past two years. There are good reasons for keeping medical data private and limiting the access. An employer may decide not to hire someone with certain diseases. An insurance company may refuse to provide life insurance knowing the disease history of a patient. Despite the paramount importance, privacy issues are not addressed adequately at the technical level and efforts to keep health data secure have often fallen short. This is because protecting privacy in the cyberspace is significantly more challenging. Thus, there is an urgent need for the development of viable protocols, architectures, and systems assuring privacy and security to safeguard sensitive and personal digital information. Outsourcing data storage and computational tasks becomes a popular trend as we enter the cloud computing era. A wildly successful story is that the company's total claims capture and control (TC3) which provides claim management solutions for healthcare payers such as medicare payers, insurance companies, municipalities, and self-insured employer health plans. TC3 has been using Amazon's EC2 cloud to process the data their clients send in (tens of millions of claims daily) which contain sensitive health information. Outsourcing the computation to the cloud saves TC3 from buying and maintaining servers, and allows TC3 to take advantage of Amazon's expertise to process and analyze data faster and more efficiently. The proposed cloud-assisted mobile health networking is inspired by the power, flexibility, convenience, and cost efficiency of the cloud-based data/computation outsourcing paradigm. We introduce the private cloud which can be considered as a service offered to mobile users. The proposed solutions are built on the service model shown in Fig. 1. A software as a service (SaaS) provider provides private cloud services by using the infrastructure of the public cloud providers

(e.g., Amazon, Google). Mobile users outsource data processing tasks to the private cloud which stores the processed results on the public cloud.

II. Cloud Computing

The Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Cloud computing is a practical approach to experience direct cost benefits and it has the potential to transform a data center from a capital-intensive set up to a variable priced environment.

The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries.

Forrester defines cloud computing as:

"A pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end-customer applications and billed by consumption.

III. Cloud Computing Challenges

The Despite its growing influence, concerns regarding cloud computing still remain. In our opinion, the benefits outweigh the drawbacks and the model is worth exploring. Some common challenges are:

1. Data Protection

Data Security is a crucial element that warrants scrutiny. Enterprises are reluctant to buy an assurance of business data security from vendors. They fear losing data to competition and the data confidentiality of consumers. In many instances, the actual storage location is not disclosed, adding onto the security concerns of enterprises. In the existing models, firewalls across data centers (owned by enterprises) protect this sensitive information. In the cloud model, Service providers are responsible for maintaining data security and enterprises would have to rely on them.

2. Data Recovery and Availability

All business applications have Service level agreements that are stringently followed. Operational teams play a key role in management of service level agreements and runtime governance of applications. In production environments, operational teams support

- Appropriate clustering and Fail over
- Data Replication
- System monitoring (Transactions monitoring, logs monitoring and others)
- Maintenance (Runtime Governance)
- Disaster recovery
- Capacity and performance management

If, any of the above mentioned services is under-served by a cloud provider, the damage & impact could be severe.

3. Management Capabilities

Despite there being multiple cloud providers, the management of platform and infrastructure is still in its infancy. Features like „Auto-scaling" for example, are a crucial requirement for many enterprises. There is huge potential to improve on the scalability and load balancing features provided today.

4. Regulatory and Compliance Restrictions

In some of the European countries, Government regulations do not allow customer's personal information and other sensitive information to be physically located outside the state or country. In order to meet such requirements, cloud providers need to setup a data center or a storage site exclusively within the country to comply with regulations. Having such an infrastructure may not always be feasible and is a big challenge for cloud providers.

IV. Proposed System

To In the PROPOSED MODEL, a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. We leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Our 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.

V. Advantages Of The Proposed System

- Security level will be increased.
- Trustworthiness will also be maintained properly.

User Registration:

If the Patients wants to access the data from the server, they should have an account with that server. Without having an account they aren't able to access the files are view the details. So first the patient will create an account with that server by providing the necessary information like Username, Password, Address and Phone number, medicines they are using and type of diagnosis and treatment that they are taking etc. Once this information are provided by the user, server will get those information and stored it into the database for future purpose.

Cloud Server:

Cloud Computing means sharing of resource. The resource will be stored in the Remote server called as Cloud Server. In our project all the patient's information will be stored in the Cloud Servers. 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.

Access Previleges:

Although the Cloud Computing is vast developing technology, In security point of view the it need more growth. To overcome this disadvantage, we implementing two types of Cloud. Once is Public Cloud and another one is Private Cloud. In Private the patient will set the access privileges' for each and every user they wish. 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'.

Data View:

The legitimate users are allowed to view the data Cloud in the Cloud Server up to their privileges'. To view the each stored in the Cloud Server, each user have to provide their authentication key then only they can able to view the data. 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.

Encryption and Decryption

MD5 has shown its promising future in fine-grained access control for outsourced sensitive data. Typically, data are encrypted by the owner under a set of attributes. The parties accessing the data are assigned access structures by the owner and can decrypt the data only if the access structures match the data attributes. public cloud returns the encrypted files which also contain "diabetes"-related files. The private cloud regenerates the update keys based on the time tags to decrypt the files. Since the decrypted results may include files of other keywords, e.g., F(wj), we let the private cloud append descriptive file identifiers, e.g., "Diabetes_10" and "Diabetes_18" to the data files before encryption.

Uml Diagrams

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems. The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

Goals:

The Primary goals in the design of the UML are as follows:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Be independent of particular programming languages and development process.
3. Provide a formal basis for understanding the modeling language.
4. Encourage the growth of OO tools market.
5. Support higher level development concepts such as collaborations, frameworks, patterns and components.

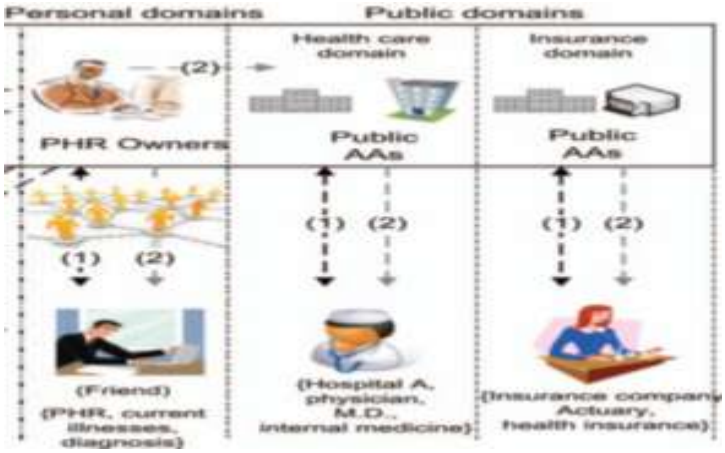

Fig 1 Architecture

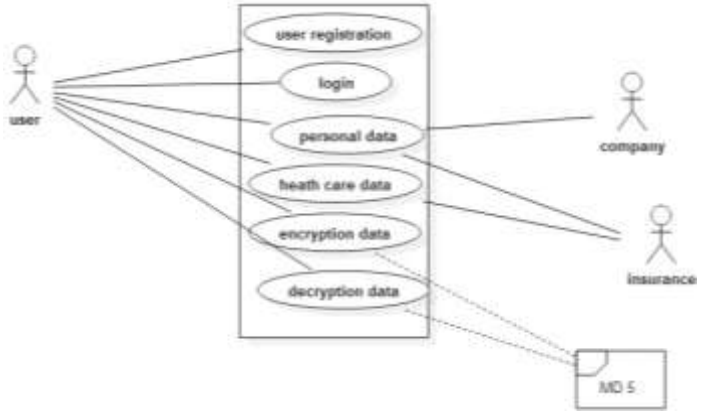

Fig 1.1 Class Diagram

VI. Conclusion

In This Paper, We Have Proposed A Novel Framework Of Secure Sharing Of Personal Health Records In Cloud Computing. Considering Partially Trustworthy Cloud Servers, We Argue That To Fully Realize The Patient-Centric Concept, Patients Shall Have Complete Control Of Their Own Privacy Through Encrypting Their PHR 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.

References

Journal Papers:

[1]. M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in SecureComm'10, Sept. 2010, pp. 89–106.

[2]. H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[3]. M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[4]. "The health insurance portability and accountability act." [Online]. Available:http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[5]. "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.

[6]. "At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded," 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26

[7]. K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001.

[8]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in IEEEINFOCOM'10, 2010.

[9]. C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.