ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2016

Attribute Based Encryption for Scalable and Secure Sharing of Cloud Computing Design and Implementation -Survey

Govardhini S, Shobana D

Assistant Professor, Dept. of CT., Sri Krishna Arts and Science College, Coimbatore, India

ABSTRACT: Personal health record (PHR) is associate rising patient-centric model of health data exchange, that's sometimes outsourced to be keep at a third party, like cloud suppliers. However, there are unit's wide privacy issues as personal health data may be exposed to those third party servers and to unauthorized parties. To assure the patients' management over access to their own PHRs, it is a promising methodology to cipher the PHRs before outsourcing. Yet, issues like risks of privacy exposure, quantifiability in key management, versa ward achieving fine-grained, cryptographically implemented information access management. Throughout this paper, we've an inclination to propose a singular patient-centric framework and a set of mechanisms for information access management to PHRs confine semi-trusted servers. For locating this disadvantage throughout this thesis projected PHR system, supported Attribute based Broadcast coding (ABBE).

KEYWORDS: PHR, Cipher, ABBE

I. INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows end-users to use applications such as data storage, email, word- processing, spreadsheets, collaboration, file conversation, social media, etc. without installing on their personal computers and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing various resources such as storage, memory, processing and bandwidth. A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc.

Depending on the type of provided capability, there are three scenarios where Clouds are used

A. **Software as a Service SaaS** is an On-demand model and offers an application, such as ERP, CRM, Google Apps etc. on demand over the internet

B. **Platform as a Service PaaS** provider sells a complete development platform including the necessary built-in services, such as MySQL database, LDAP, Net Beans software, on demand over the network

C. **Infrastructure as a Service IaaS** is a foundation layer for other two delivery models and offers hardware and software infrastructure components, such as compute, storage, system etc.,

DOI: 10.15680/IJIRCCE.2016. 0407203

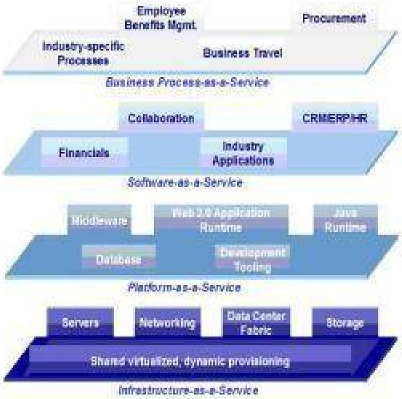

Figure 1. Different services provided by cloud

AWS offers two cloud environments--Amazon Elastic Compute Cloud (EC2) and Virtual Private Cloud (VPC). EC2 is intended for delivering services to Internet users without data center integration. Web servers offering content is one example. VPC is better suited for integrating with your corporate network and users. By default, the VPC has no connectivity to the Internet unless explicitly configured.
Amazon makes data center integration possible by letting IT:

- Create subnets using private addresses in the RFC1918 space
- Establish custom route tables
- Deploy network access lists (ACLs) that provide protection at the subnet level
- Pass configuration information to VMs using DHCP option sets

- Connect securely to your data center using IPsec over the Internet or dedicated connections from AWS data centers to your data center

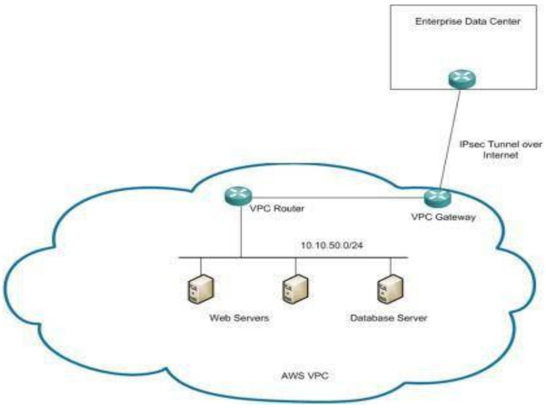

Figure 2 shows acls method

VPC has limitations that administrators should understand. The VPC supports only RFC1918 space within the VPC. If this presents problems for your network, you can use NAT in your data center to make the VPC appear to be numbered from another address space. AWS built the VPC to scale to massive size. To accomplish this feat, the engineers chose a Layer 3 (that is, IP) foundation for networking. A ramification of this decision is that VPC does not support broadcast and VLANs. Traffic separation must be done at the subnet level. Since enterprise networks rely heavily on VLANs for separations, this is a significant problem if you expect to port VLAN-centric designs to the cloud.

Let's turn to an example. You want to provision a set of VMs in the cloud to run your Web-based expense reporting system. Only users on your corporate network need to access the application. You need two Web servers and one database server. Data between your data center and your VPC will be encrypted using the IPSec protocol

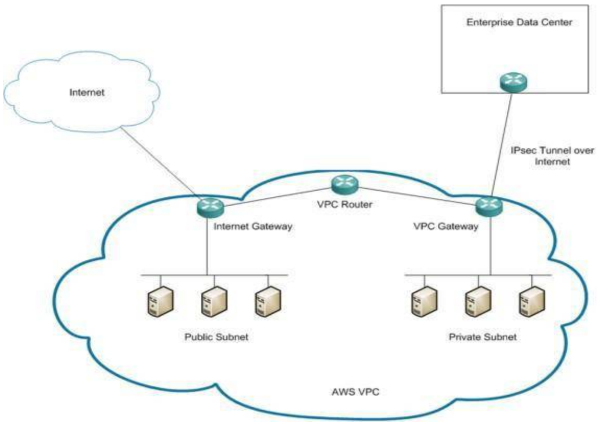

Figure 3 show VPC based data forwading in cloud

Now data center has been extended to the cloud. The users will access the expense reporting application no differently than they would applications hosted in your data center. This is useful for deploying e-commerce and other customer-facing services.

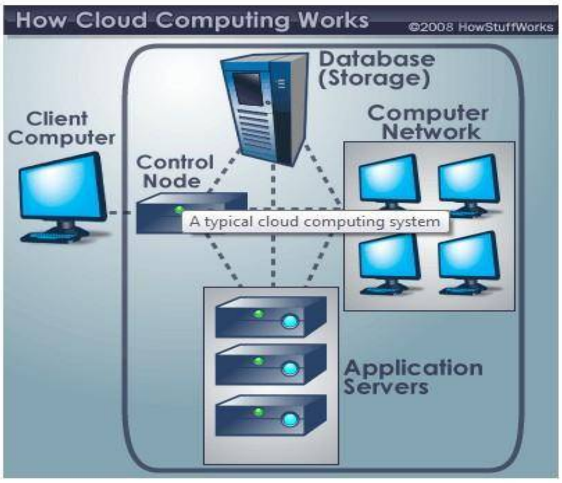

Figure 4 Cloud computing system

Cloud computing means storing and accessing data and programs over the internet instead of using computer's hardware and software. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. Personal Health Record (PHR) service is an emerging model for health information exchange. It allows 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. Advance technology of cloud computing PHR has undergone substantial changes. 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.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. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client's data, a novel patient centric framework is used.

The definition of PHR is heterogeneous and evolving. A personal health record (PHR) is simply a collection of information about a person's health. It is a tool for the excellent management of the health. J. Benaloh, Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. But it is a single data owner scenario and thus it is not easy to add categories. C.Dong, Shared and Searchable Encrypted Data for untreated Servers, has explored that the data encryption scheme does not require a trusted data server. 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. Public key Encryption (PKE) based scheme is one of the encryption method used for protecting data from third parties. But it has high key management overhead, or requires encrypting multiple copies of a file using different user's keys. Attribute based encryption is based on some access policies. These access policies are expressed based on the attribute of users or data which help to share PHR among set of users by encrypting the file under a set of attributes. Only authorized users with satisfying this access policy can access the PHR data. The main property of ABE is preventing against user collusion and the owner is not required to know the ACL.

In recent years, personal health record (PHR) has e- merged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each

patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed in .While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third- party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to expo- sure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization.

To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A feasible and promising approach would be to en- crypt the data before outsourcing. Basically, the PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the user s that are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. However, the goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users‟ access requests are generally unpredictable, it is difficult for an owner to determine a list of them. On the other hand, different from the single data owner scenario considered in most of the existing works in a PHR system, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner who's PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority (i.e.,cause the key escrow problem). In this paper, 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-based encryption (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. However, to integrate ABE into a large -scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions: (1) We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To ad- dress the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications requirements, while incurring minimal key management overhead for both owners and users in the system.

In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios. In the public domain, we use multi-authority ABE (MA- ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. Furthermore, we enhance MA-ABE by putting forward an efficient and on-demand user/attribute revocation scheme, and prove its security under standard security assumptions. In this way, patients have full privacy control over their PHRs. We provide a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage and key management. We also compare our scheme to several previous ones in complexity, scalability and security. Furthermore, we demonstrate the efficiency of our scheme by implementing it on a modern workstation and performing experiments/simulations.

Compared with the preliminary version of this paper there are several main additional contributions:

- We clarify and extend our usage of MA-ABE in the public domain, and formally show how and which types of user-defined file access policies are realized.
- We clarify the proposed revocable MA-ABE scheme, and provide a formal security proof for it.

- We carry out both real-world experiments and simulations to evaluate the performance of the proposed solution in this paper.

Patient centric medical records information exchange is model for the sharing of medical records, which allows patient to create, manage and control his/her medical information in centralized place through the web or cloud. Patient can now share his/her medical records effectively with a wide range of users such as family members, friends and doctors. Cloud Computing made lots of attraction, because of there is provision of storage as service and software as service, by which software service providers can enjoy the virtually infinite and elastic storage and computing resources. As such, the providers are more and more willing to shift their storage and application services into the cloud like Microsoft and Amazon, instead of building specialized data centers, in order to lower their operational cost .While it is exciting to have these services in the cloud for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about the privacy of patients' personal health data and who could gain access to the medical records when they are stored in a cloud server. Since patients lose physical control to their own personal health data, directly placing those sensitive data under the control of the servers cannot provide strong privacy assurance at all. While going for cloud computing storage, the data owner and cloud servers are in two different domains. On one hand, cloud servers are not entitled to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of data owner. Storing personal medical records on the cloud server leads to need of Encryption mechanism to protect the medical health record, before outsourcing to the cloud.

II. CONCLUSION

To deal with the potential risks of privacy exposure, instead of letting the service providers encrypt patients' data, medical records sharing services should give patients (patient / medical record owners) full control over the selective sharing of their own medical data. To this end, the medical records should be encrypted in addition to traditional access control mechanisms provided by the server we use Java Paring Based Cryptography library (jPBC) for the implementation of KP-ABE and MA-ABE. In this paper, we discussed the design and Implementation detail for the of the proposed framework.

Hence, our technology can be easily adopted in a cloud computing environment to replace the traditional Hash-based solution. More importantly, we proposed and quantified a new audit approach based on probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services.

REFERENCES

1. http://aspe.hhs.gov/admnsimp/pl104191.htm, *104th United States Congress, Health Insurance Portability and Accountability Act of1996*.
2. Tim Mather, SubraKumaraswamy, and ShahedLatif,Cloud Security and Privacy, *Published by O Reilly Media,Inc.*, 2009.
3. http://security.setecs.com, Security Architecture for Cloud Computing Environments, *White paper*, 2011.
4. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records,"
5. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data,"

BIOGRAPHY

Govardhini S is a Assistant professor in the computer Technology Department, College of Sri Krishna Arts and Science college, Coimbatore, She received Master of Computer Application (MCA) degree in 2013 Anna University Her research interests are Computer Networks.

Shobana D is a Assistant professor in the Information Technology Department, College Sri Krishna Arts and Science college, Coimbatore, She received Master of Computer Application (MCA) degree Bharathiyar University Her research interests are Computer Networks