International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Secure Patient-Centric PHRs management in Cloud Computing using ABE

Prathipati Srinu[*1] and J. Raja Rajeswari[#2]

Student, Dept of Computer Science, Jogaiah Institute of Technology and Sciences College of Engineering, A.P, India

Asst Professor, Dept of Computer Science, Jogaiah Institute of Technology and Sciences College of Engineering, A.P, India

p.srinu.1262@gmail.com

rajeswari506@gmail.com

Abstract— The storage and retrieval of Patient Health Records (PHR) is one of the most important applications of Data Sharing in Cloud. It maintains the patient's personal and diagnosis information. At most privacy and security measures are required for the safe retrieval of these records. The sensitive attributes are being protected by the privacy mechanism. To protect the data from public access, the security schemes are used. Only Authorized individuals are allowed to access the data. Each party is assigned with access permission for a set of attributes. Data owners update the patient data into third party cloud data centers. The attribute based encryption (ABE) scheme is used to secure these patient records. The same data values are accessed by multiple owners. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism due to its vast access. The MA-ABE model is not tuned to provide identity based access mechanism. Distributed storage model is not supported in the MA-ABE model. The proposed system is designed to provide identity based encryption facility. The attribute based encryption scheme is enhanced to handle distributed attribute based encryption process. Data update and key management operations are tuned for multi user access environment.

Key Words: Personal health records, cloud computing, multi-authority attribute-based encryption, distributed environment, attribute based encryption

I. INTRODUCTION

Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable, confidential and accountable 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. The underlying details of how it is achieved are hidden from the user. The data and the services provided reside in massively scalable data centers and can be ubiquitously accessed from any connected device all over the world.

In simple words, cloud computing is nothing but the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Fig 1 cloud computing

ADVANTAGES OF CLOUD

Enterprises would need to align their applications, so as to exploit the architecture models that Cloud Computing offers. Some of the typical benefits are listed below:

Self Healing: Any application or any service running in a cloud computing environment has the property of self healing. In case of failure of the application, there is always a hot backup of the application ready to take over without disruption. There are multiple copies of the same application - each copy updating itself regularly so that at times of failure there is at least one copy of the application which can take over without even the slightest change in its running state.

Multi-Tenancy: With cloud computing, any application supports multi-tenancy - that is multiple tenants at the same instant of time. The system allows several customers to share the infrastructure allotted to them without any of them being aware of the sharing. This is done by virtualizing the servers on the available machine pool and then allotting the servers to multiple users. This is done in such a way that the privacy of the users or the security of their data is not compromised.

Linearly Scalable: Cloud computing services are linearly scalable. The system is able to break down the workloads into pieces and service it across the infrastructure. An exact idea of linear scalability can be obtained from the fact that if one server is able to process say 1000 transactions per second, then two servers can process 2000 transactions per second.

Service-Oriented: Cloud computing systems are all service oriented - i.e. the systems are such that they are created out of other discrete services. Many such discrete services which are independent of each other are combined together to form this service. This allows re-use of the different services that are available and that are being created. Using the services that were just created, other such services can be created.

Reduced Cost: There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage; the infrastructure is not purchased thus lowering maintenance. Initial expense and recurring expenses are much lower than traditional computing.

Increased Storage: With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality. Sudden workload spikes are also managed effectively & efficiently, since the cloud can scale dynamically.

Virtualized: The applications in cloud computing are fully decoupled from the underlying hardware. The cloud computing environment is a fully virtualized environment.

Flexible: Another feature of the cloud computing services is that they are flexible. They can be used to serve a large variety of workload types - varying from small loads of a small consumer application to very heavy loads of a commercial application. This is an extremely important characteristic. With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical. Cloud computing stresses on getting applications to market very quickly, by using the most appropriate building blocks necessary for deployment.

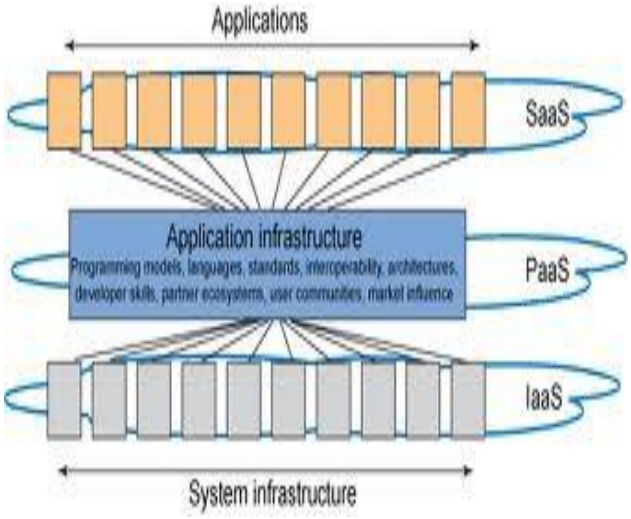

Fig 2: Components of Cloud

II. DATA PROTECTION DIMENSION

This paper distinguished three classifications of security solutions that may be useful in relation to cloud computing. We will discuss these security solutions below and relate them to cloud computing.

1) System Solutions: These are based on the physical layer of an information system, directly manipulating the software and hardware in order to achieve security. As system based solutions are responsible for the security at the lower levels of the technology stack, these security mechanisms enable the use of other security solutions, like the behavioral and hybrid solutions discussed below. System based solutions such as cryptography act as building blocks for behavioral solutions. An example of a system solution is an Intrusion Detection System (IDS), which detects security breaches by monitoring data transfers and executions of functionality.

2) Behavioral Solutions: These act on a higher plane of abstraction than the system solutions described above. As the name says, the behavioral solutions are focused on the behavior of the users of an information system. The behavior is controlled in the form of policies-based solutions which limit the user's access to an information system, and trust-

based solutions in where other security mechanisms are only needed if the user is not trusted enough.

3) Hybrid Solutions: These are a category of solutions that combine system and behavioral solutions. Examples of hybrid solutions are authentication and authorization mechanisms.

III. PERSONAL HEALTH RECORD (PHR)

In recent years, personal health record (PHR) has emerged 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 Health Vault.

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 exposure 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.

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. 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.

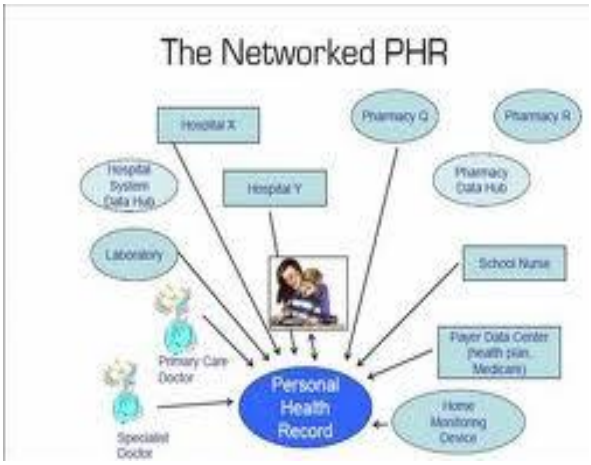

Fig 3: Personal Health Records usage

IV. FRAMEWORK FOR PATIENT-CENTRIC, SECURE AND SCALABLE PHR SHARING

In this section, we describe our novel patient-centric secure data sharing framework for cloud-based PHR systems. We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners‟ PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners‟ data. A typical PHR system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative PHR systems including Indivo, an open-source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way.

In this paper, we consider the server to be semi trusted, i.e., honest but curious. That means the server will try to find out as much secret information in the stored PHR files as possible,

but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

To achieve "patient-centric" PHR sharing, a core requirement is that each patient can control who are authorized to access to her own PHR documents. Especially, user controlled read/write access and revocation are the two core security objectives for any electronic health record system. The security and performance requirements are summarized as follows:

1) Data Confidentiality: Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.

2) On-demand revocation: Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. There is also user revocation, where all of a user's access privileges are revoked.

3) Write access control: We shall prevent the unauthorized contributors to gain write-access to owners‟ PHRs, while the legitimate contributors should access the server with accountability.

4) Scalability, efficiency and usability: The PHR system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners‟ efforts in managing users and keys should be minimized to enjoy usability.

V. 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.

VI. REFERENCES

[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] http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp
[5] http://www.ihealthbeat.org/Articles/2009/4/8/.
[6] 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 IEEE INFOCOM'10, 2010.
[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.
[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010..

PRATHIPATI SRINU received her B.Tech Degree in IT from NOVA COLLEGE of ENGGENIRING AND Technology Vegavaram, West Godavari (Dt), in 2012. Presently, he is pursuing the M.Tech degree in CSE from JOGAIAH INSTITUTE OF TECHNOLOGY AND SCIENCES COLLEGE OF ENGINEERING Kalagampudi. West Godavari (Dt).

J.RAJA RAJESWARI received the M.Tech degree from Jogaiah Institute of Technology And Sciences Kalagampudi West Godavari (Dt), in 2013.. Currently She is working as ASSISTANT Professor in JITS Engineering College, Kalagampudi. She has three years of experience in teaching.