

Securing Patient Health Information in Cloud Environment

¹Geetha*, Assistant Professor, Mahendra Engineering College for Women, Tamilnadu, India

²Dr. M. Thangamani, Assistant Professor, Kongu Engineering College, Tamilnadu, India

ABSTRACT

Patient Health Records (PHR) is maintained in the centralized server to maintain the patient's personal and diagnosis information. The patient records should be maintained with privacy and security. The privacy mechanism protects the sensitive attributes. The security schemes are used to protect the data from public access. Each authority is assigned with access permission for a set of attributes. Cloud computing environment supports storage spaces for patient health record management process. Data owns update the patient data into third party cloud data centers. The attribute based encryption (ABE) scheme is used to secure the patient records for selected sensitive attributes. Multiple owners can access the same data values. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism. The MA-ABE model is not tuned to provide identity based access mechanism. Distributed storage model is not supported in the MA-ABE model. These systems are designed to provide identity based encryption facility. Data update and key management operations are tuned for multi user access environment.

Keywords: PHR, ABE, MA-ABE

1. INTRODUCTION

A key differentiating element of a successful information technology (IT) is its ability to become a true, valuable, and economical contributor to cyber infrastructure. Cloud computing embraces cyber infrastructure, and builds upon decades of research in virtualization, distributed computing, grid computing, utility computing, and, more recently, networking, web and software services. It implies service oriented architecture, reduced information technology Over head for the end-user, greater flexibility, reduced total cost of ownership, on demand services and many other things.

1.1 Cyber Infrastructure

Cyber infrastructure makes applications dramatically easier to develop and deploy, thus expanding the feasible scope of applications possible within budget and organizational constraints, and shifting the scientists and engineers effort away from information technology

development and concentrating it on scientific and engineering research. Cyber infrastructure also increases efficiency, quality, and reliability by capturing commonalities among application needs, and facilitates the efficient sharing of equipment and services.

Today, almost any business or major activity uses, or relies in some form, on IT and IT services. These services need to be enabling and appliance-like, and there must be an economy-of-scale for the total-cost-of-ownership to be better than it would be without cyber infrastructure. Technology needs to improve end user productivity and reduce technology-driven overhead. Unless IT is the primary business of an organization, less than 20% of its efforts not directly connected to its primary business should have to do with IT overhead, even though 80% of its business might be conducted using electronic means.

1.2 Cloud Concepts

A powerful underlying and enabling concept is computing through service-oriented architectures (SOA) – delivery of an integrated and orchestrated suite of functions to an end-user through composition of both loosely and tightly coupled functions, or services – often network based. Related concepts are component-based system engineering, orchestration of different services through workflows, and virtualization.

1.3 Cloud Components

The key to a SOA framework that supports workflows is componentization of its services, an ability to support a range of couplings among workflow building blocks, fault-tolerance in its data- and process-aware service-based delivery, and an ability to audit processes, data and results, that is collected and use provenance information. Component-based approach is characterized by reusability, substitutability, extensibility and scalability, customizability and composability. There are other characteristics that also are very important. Those include reliability and availability of the components and services, the cost of the services, security, total cost of ownership, economy of scale, and so on. In the context of cloud computing we distinguish many categories of components: from differentiated and undifferentiated hardware, to general purpose and specialized software and applications, to real and virtual images, to environments, to no-root differentiated resources, to workflow-based environments and collections of services, and so on.

2. RELATED WORK

Identity-based encryption is type of public key encryption in which the public key of a user is some unique information [1] about the identity of the user. Lewko and Waters [2,3], used a Multi-Authority Attribute-Based Encryption system. In this case, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters.

The application of information technology to healthcare has become increasingly important in many countries in the recent years [4]. There are continuing efforts on national and

international standardization for interoperability and data exchange. Many different application scenarios are envisaged in electronic healthcare, electronic health records, accounting and billing, medical research, and trading intellectual property. In particular e-health systems like electronic health records (EHRs) are believed to decrease costs in healthcare and to improve personal health management in general. They also include specifications for security and privacy aspects; their main focus is currently the interoperability and definition of common document exchange formats and nomenclature of medical data objects.

Dong.C et.al [5] introduced the scheme supports keyword search which enables the server to return only the encrypted data that satisfies an encrypted query without decrypting it. The patient's medical record may threaten the accessibility of the information and compromise patients' privacy [6].

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange [7]. A PHR service allows a patient to create, manage, and control her personal health data in a centralized place through the web, from anywhere and at any time, which has made the storage, retrieval, and sharing of the the medical information more efficient. Especially, each patient has the full control of her medical records and can effectively share her health data with a wide range of users, including staffs from healthcare providers, and their family members or friends. In this way, the accuracy and quality of care are improved, while the healthcare cost is lowered.

Cloud computing has attracted a lot of attention because it provides storage-as-a-service and software-as-a-service, by which software service providers can enjoy the virtually infinite and elastic storage and computing resources. As such, the PHR providers are more and more willing to shift their PHR storage and application services into the cloud instead of building specialized data centers, in order to lower their operational cost. Two major cloud platform providers, Google and Microsoft are both providing their PHR services. Different techniques based on the attribute-based encryption [8] have been designed to secure the cloud storage

3. PROPOSED ARCHITECTURE

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 and personal domains (PSDs) according to the different users data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner and they make accesses to PHRs based on access rights assigned by the owner.

The PHR security system is adapted to policy based and identity based security systems. The distributed ABE model is adopted to support multiple server frameworks. The data owners can change the access policies dynamically. The system reduces the key management and revocation complexity. The system is designed to manage patient health records under cloud data

centers. Multi party based data ownership and access mechanism is used in the system. Different key values are used to secure different attributes. The system is divided into six major modules. They are data owner, cloud provider, key management, security process, authority analysis and client.

4. IMPLEMENTATION AND RESULTS

The data owner module is designed to handle data update process. The cloud data provider module is designed to store and maintain the patient health records. The key management module is designed to handle the key update and distribution process. The security process module is designed to perform the attribute based encryption process. The authority analysis module is designed to verify the data access. The client module is designed to perform the data retrieval process.

Data Owner: The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities. Fig.1 shows the patient attributes and values. Fig.3 and Fig.4 shows the medical and insurance details of the patients.

The screenshot displays a web application window titled "D:\MECW-BTech\MTBatch\Project\User\.: Patient Details". The main content area is titled "Patient Details" in a pink, cursive font. Below the title, there is a form with the following fields and values:

| Attribute | Value |
|-------------|--------|
| User ID | 200 |
| User Name | Aliya |
| Age | 26 |
| Sex | Female |
| Blood Group | A +ve |
| Height | 158 |
| Weight | 60 |

At the bottom of the form, there are two buttons: "Save" and "Back". A small dialog box is overlaid on the right side of the form, displaying the message "Patient details updated successfully" with an "OK" button.

Fig 1. Patient Details

Cloud Provider The cloud provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are also maintained under the cloud provider. Fig.2 represents the screen shot of cloud data provider.

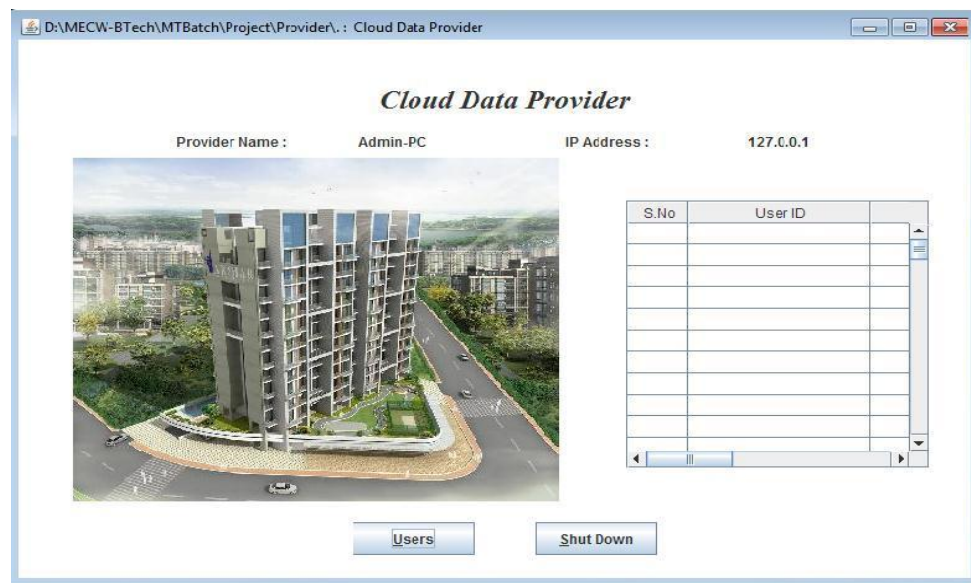


Fig.2 Cloud Data Provider

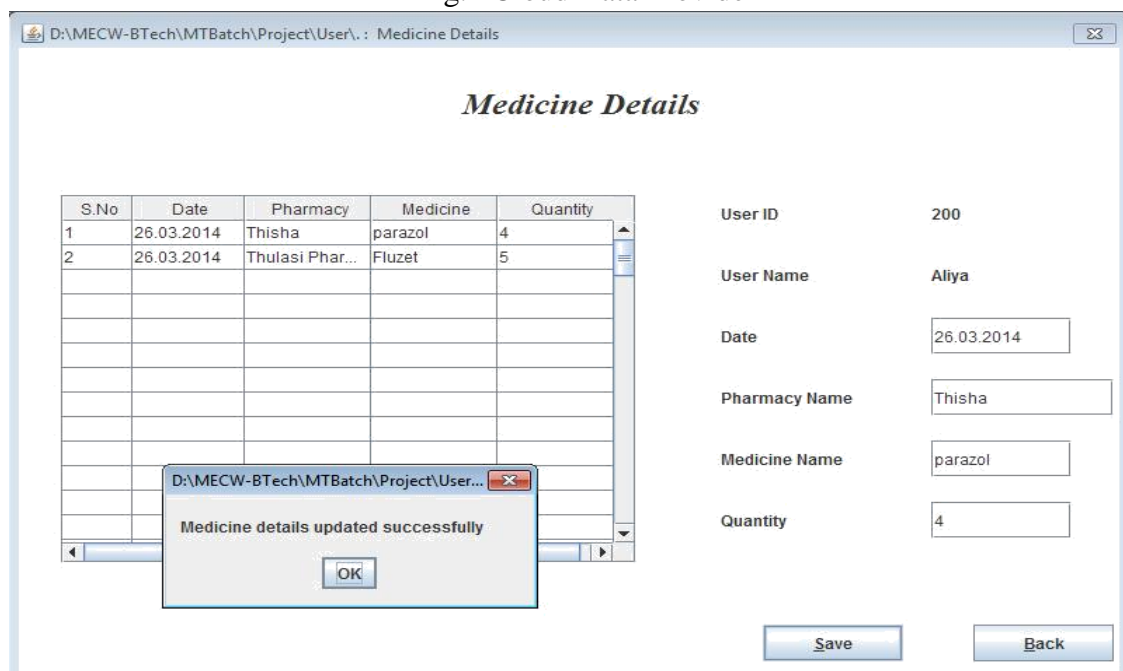


Fig.3 Patent medicine details

Key Management: The key management module is designed to manage key values for different authorities. Key values are uploaded by the data owners. Key management process includes key insert and key revocation tasks. Dynamic policy based key management scheme is used in the system. Fig.5 represents key management module view.

Security Process: The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data decryption is performed under the user environment.

Authority Analysis: Authority analysis module is designed to verify the users with their roles. Authority permissions are initiated by the data owners. Authority based key values are issued by the key management server. The key and associated attributes are provided by the central authority.

Client: The client module is used to access the patients. Personal and professional access models are used in the system. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process.

Security for E-Health Records: PHR system consists multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data that is they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. Users access the PHR documents through the server in order to read or write to someones PHR, and a user can simultaneously have access to multiple owners' data. A typical PHR system uses standard data formats. 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.

PHR Security with MA-ABE: The main goal 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 and personal domains (PSDs) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner and they make accesses to PHRs based on access rights assigned by the owner.

PHR Encryption and Access: The owners upload ABE-encrypted PHR files to the server. Each owners PHR file is encrypted both under a certain finegrained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root.

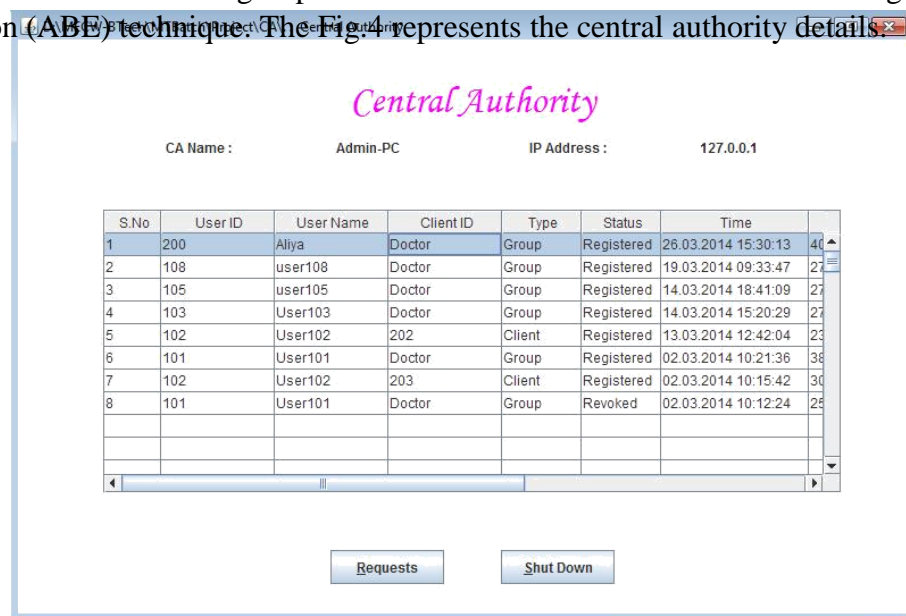
User Revocation: There are several possible cases: Revocation of one or more role attributes of a public domain user, Revocation of a public domain user which is equivalent to

revoking all of that users attributes. These operations are done by the AA that the user belongs to, where the actual computations can be delegated to the server to improve efficiency. Revocation of a personal domain users access privileges, Revocation of a personal domain user. These can be initiated through the PHR owners client application in a similar way.

Enhancing MA-ABE for User Revocation: To revoke a user in MA-ABE, one needs to find out a minimal subset of attributes (γ) such that without it the user's secret key's access structure (A_u) will never be satisfied. Because our MA-ABE scheme requires conjunctive access policy across the AAs, it suffices to find a minimal subset by each AAk without which A_{uk} will not be satisfied, and then compute the minimal set (γ_{kmin}) out of all γ_k . The AAkmin will initiate the revocation operation.

Handle Dynamic Policy Changes: This scheme should support the dynamic add or modify or delete of part of the document access policies or data attributes by the owner. If a patient does not want doctors to view her PHR after she finishes a visit to a hospital, she can simply delete the ciphertext components corresponding to attribute "doctor" in her PHR files. Adding and modification of attributes or access policies can be done by proxy reencryption techniques; however they are expensive. To make the computation more efficient, each owner could store the random number s used in encrypting the FEK3 of each document on her own computer, and construct new ciphertext components corresponding to added or changed attributes based on s .

The cloud data security system is designed to protect the patient health records. The patient health records are secured using the attribute based encryption techniques. In this system construct a cloud data center to share Patient Health Records (PHR) and provide privilege based access with user and user group level. It also secures the data values using Attribute Based Encryption (ABE) technique. The Fig.4 represents the central authority details.



| S.No | User ID | User Name | Client ID | Type | Status | Time |
|------|---------|-----------|-----------|--------|------------|---------------------|
| 1 | 200 | Aliya | Doctor | Group | Registered | 26.03.2014 15:30:13 |
| 2 | 108 | user108 | Doctor | Group | Registered | 19.03.2014 09:33:47 |
| 3 | 105 | user105 | Doctor | Group | Registered | 14.03.2014 18:41:09 |
| 4 | 103 | User103 | Doctor | Group | Registered | 14.03.2014 15:20:29 |
| 5 | 102 | User102 | 202 | Client | Registered | 13.03.2014 12:42:04 |
| 6 | 101 | User101 | Doctor | Group | Registered | 02.03.2014 10:21:36 |
| 7 | 102 | User102 | 203 | Client | Registered | 02.03.2014 10:15:42 |
| 8 | 101 | User101 | Doctor | Group | Revoked | 02.03.2014 10:12:24 |

Fig.6 Central Authority

5. CONCLUSION AND FUTURE DIRECTION

The patient health records are maintained in a data server under the cloud environment. Public and personal access models are designed with security and privacy enabled mechanism. The system can be enhanced with the integrity analysis mechanism can be integrated with the system to detect data errors.

References

1. A. Boldyreva, V. Goyal and V. Kumar, Identity-Based Encryption with Efficient Revocation, Proc. 15th ACM Conf. Computer and Communication Security, pp.417-476, 2008.
2. A. Lewko and B. Waters, Decentralizing Attribute-Based Encryption, EUROCRYPT: Proc. 30th Ann. International conference on Theory and Applications of Cryptographic Techniques: Advances in Cryptology, pp. 568-588, 2011.
3. A. Sahai, B. Waters and J. Bethencourt, Cipher text-policy attribute-based encryption, in IEEE S&P, pp. 321-334, 2007.
4. A.R. Sadeghi, H. Lo hr and M. Winandy, Securing the E-Health Cloud, Proc. first ACM International Health Informatics Symp., pp. 220-229, 2010.
5. C. Dong, G. Russello, and N. Dulay, Shared and Searchable Encrypted Data for Untrusted Servers, Journal of Computer Security, vol. 19, pp. 367-397, 2010.
6. Kohane. I.S, Mandl and P. Szolovits, Public Standards and Patients Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, 2001.
7. . K. Ren, M. Li, S. Yu and W. Lou, (2010) „Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth ICST Conf. Security and Privacy in Communication Networks, pp. 89-106, 2010.
8. Kushal P. Kulkarni and A.M.Dixit, Privacy Preserving Health Record System in Cloud Computing using Attribute based Encryption, International Journal of Computer Applications, Vol.122, No.18, pp.6-11, 2015.

Authors Biography



Ms. S. Geeitha has completed Master of Engineering in Computer Science and Engineering in Anna University Application. Her research expertise covers Medical data mining, machine learning, cloud computing, big data, fuzzy, soft computing and ontology. She has presented 10 papers in national

and international conferences in the above fields. She is currently working as Assistant Professor in Mahendra Engineering College for Women.



Dr. M. Thangamani possesses nearly 20 years of experience in research, teaching, consulting and practical application development to solve real-world business problems using analytics. Her research expertise covers Medical data mining, machine learning, cloud computing, big data, fuzzy, soft computing, ontology development, web services and open source software. She has published nearly 70 articles in refereed and indexed journals, books and book chapters and presented over 67 papers in national and international conferences in the above field. She has delivered more than 60 Guest Lectures in reputed engineering colleges on various topics. She has got best paper awards from various education related social activities in India and Abroad. She has organized many self-supporting and government sponsored national conference and Workshop in the fields of data mining, big data and cloud computing. She continues to actively serve the academic and research communities. She is on the editorial board and reviewing committee of leading research journals, which includes her nomination as the Associate Editor to International Journal of Entrepreneurship and Small & Medium Enterprises at Nepal and on the program committee of top international data mining and soft computing conferences in various countries. She is also seasonal reviewer in IEEE Transaction on Fuzzy System, international journal of advances in Fuzzy System and Applied mathematics and information journals. She has been nominated as chair and keynote speaker in international conferences in India and countries like Malaysia, Thailand and China. She has Life Membership in ISTE, Member in CSI, International Association of Engineers and Computer Scientists in China, IAENG, IRES, Athens Institute for Education and Research and Life member in Analytical Society of India. She is currently working as Assistant Professor at Kongu Engineering College at Perundurai, Erode District.