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.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Multi Organization Records Sharing in Cloud Computing Using Attribute Based Encryption

Sampath.N[1]

ME, Department of CSE, SSM College of Engineering, Komarapalayam, Tamil Nadu, India[1]

ABSTRACT: Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes are used to control access from untrusted users or servers to protect single users or combinations of multi users called organization resources. But, in internal organization for all user levels have same and single access control method maintained by cloud providers and didn't have data confidentiality between user levels (fine grained access problem). This method used to access only the single dataset or local dataset from the cloud computer.

In proposed, to achieve fine-grained and scalable data access control, using attribute-based encryption (ABE) techniques to encrypt each file and greatly reduces the key management complexity for owners and users. Also, focus on the multiple data owner scenario for data sharing between multi organizations using the advanced encryption standard (AES) algorithm and enables the global dataset sharing. Using global Resource Description Framework (RDF) analyze its performance, security and computational complexity.

KEYWORDS: Personal health records, data privacy, fine-grained access control, ABE, OPEX.

I. INTRODUCTION

Cloud computing, or the cloud, is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet used for sharing the resources. Cloud computing is a term without a commonly accepted unequivocal scientific or technical definition. In science, cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The phrase is also, more commonly used to refer to network-based services which appear to be provided by real server hardware, which in fact are served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user arguably rather like a cloud. The popularity of the term can be attributed to its use in marketing to sell hosted services in the sense of application service provisioning that run client server software on a remote location.

Cloud computing relies on sharing of resources to achieve coherence and economies of scale similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. The cloud also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility, which serves Indian users during Indian business hours with a specific application (e.g. email) while the same resources are getting reallocated and serve North American users during North America's business hours with another application (e.g. web server). This approach should maximize the use of computing powers thus reducing environmental damage as well since less power, air conditioning, Track space, etc. is required for a variety of functions. The term "moving to cloud" also refers to an organization moving away from a traditional CAPEX model (buy the dedicated hardware and depreciate it over a period of time) to the OPEX model (use a shared cloud infrastructure and pay as you use it).

Although the great benefits brought by cloud computing paradigm are exciting for IT companies, academic researchers, and potential cloud users, security problems in cloud computing become serious obstacles which, without being appropriately addressed, will prevent cloud computing extensive applications and usage in the future. One of the prominent security concerns is data security and privacy in cloud computing due to its Internet-based data storage and management.

Objective

Cloud computing brings the “pay as you go” model to data centers in particular, the infrastructure as a service (iaas) model allows clients to dynamically scale up/down to as many machines as needed inside the cloud. A major hurdle to the widespread adoption of this model is security, as customers often want to export sensitive data and computation into the cloud.

To realize fine-grained access control, the traditional public key encryption (PKE)-based schemes, [5] either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. To improve upon the scalability of the above solutions, one-to-many encryption methods such as attribute-based encryption ABE can be used.

II. PROBLEM DESCRIPTION

The major problem that occurred in the cloud computing model is that the export the user's sensitive data to public that create a bad opinion about this new computing technology. Data confidentiality is not the only security requirement. Flexible and fine-grained access control is also strongly desired in the service-oriented cloud computing model. For example: A health-care information system on a cloud is required to restrict access of protected medical records to eligible doctors and a customer relation management system running on a cloud may allow access of customer information to high-level executives of the company only. In these cases, access control of sensitive data is either required by legislation (e.g., HIPAA) or company regulations [2]. So the cloud providers basically use KP-ABE to detect those problems and solve by different algorithms like MA-ABE, RNS scheme, NGS schemes. Not only these fine grained access and control sensitive data from untrusted users, but also using attribute based encryption the multi organization sharing also big challenges. i.e., using this KP-ABE, data sharing between different organizations is fully stopped and every time the resource owner must be in online to grant the permission to access by the other organization peoples.

However, there are several common drawbacks of the above works:

First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure [1]. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys. In fact, different organizations usually form their own (sub) domains and become suitable authorities to define and certify different sets of attributes belonging to their (sub) domains (i.e., divide and rule).

Second, there still lacks an efficient and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, which are essential parts of secure PHR sharing [3].

Third, most of the existing works do not differentiate between the personal and public domains (PUDs), which have different attribute definitions, key management requirements, and scalability issues [5].

Finally, ABE schemes process give permission for same organization people can access their data from the cloud. When data sharing concept occur this technology came failure. In this ABE method can't collaborate the different organization database to exchange their information's in cloud computing [2].

III. OVERVIEW OF THE PROPOSED WORK

Attribute-Based Encryption

The notion of ABE was first introduced by Sahai and Waters as a new method for fuzzy identity-based encryption. In the ABE scheme, cipher texts are not encrypted to one particular user as in traditional public key cryptography. Rather, both cipher texts and users' decryption keys are associated with a set of attributes or a policy over attributes. A user is able to decrypt a cipher text only if there is a match between his decryption key and the cipher text. ABE schemes are classified into key-policy attribute-based encryption (KP-ABE) and cipher text-policy attribute-based encryption (CP-ABE), depending how attributes and policy are associated with cipher texts and users' decryption keys [2].

In a KP-ABE scheme a cipher text is associated with a set of attributes and a user's decryption key is associated with a monotonic tree access structure. Only if the attributes associated with the cipher text satisfy the tree access structure, can the user decrypt the cipher text. In a CP-ABE scheme the roles of cipher texts and decryption keys are switched; the cipher text is encrypted with a tree access policy chosen by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. As long as the set of attributes associated with a decryption key satisfies the tree access policy associated with a given cipher text, the key can be used to decrypt the cipher text. Since users decryption keys are associated with a set of attributes, CP-ABE is conceptually closer to traditional access control models such as Role-Based Access Control (RBAC). Thus, it is more natural to apply CP-ABE, instead of KP-ABE, to enforce access control of encrypted data

ABE for Fine-Grained Data Access Control, number of works used ABE to realize fine-grained access control for outsourced data. Especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs).However, the cipher text length grows linearly with the number of unrevoked users. A variant of ABE that allows delegation(rules) of access rights is proposed for encrypted EHRs.ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones or Ecard so that EMR could be accessed when the health provider is offline.

Proposed schemes:

Access control models have been the focus of recent research, including approaches in which the access control model is expressed in terms of tuples that specify who can access which schema element, what type of access is allowed, and how the access rights propagate on the tree. To security purpose a global resource attribute-set-based encryption scheme for access control in cloud computing. Global resource attribute-set-based encryption extends the ciphertext-policy attribute- set-based encryption (CP-ASBE, or ASBE for short) scheme with a hierarchical structure of system users, so as to achieve scalable, flexible and fine-grained access control.

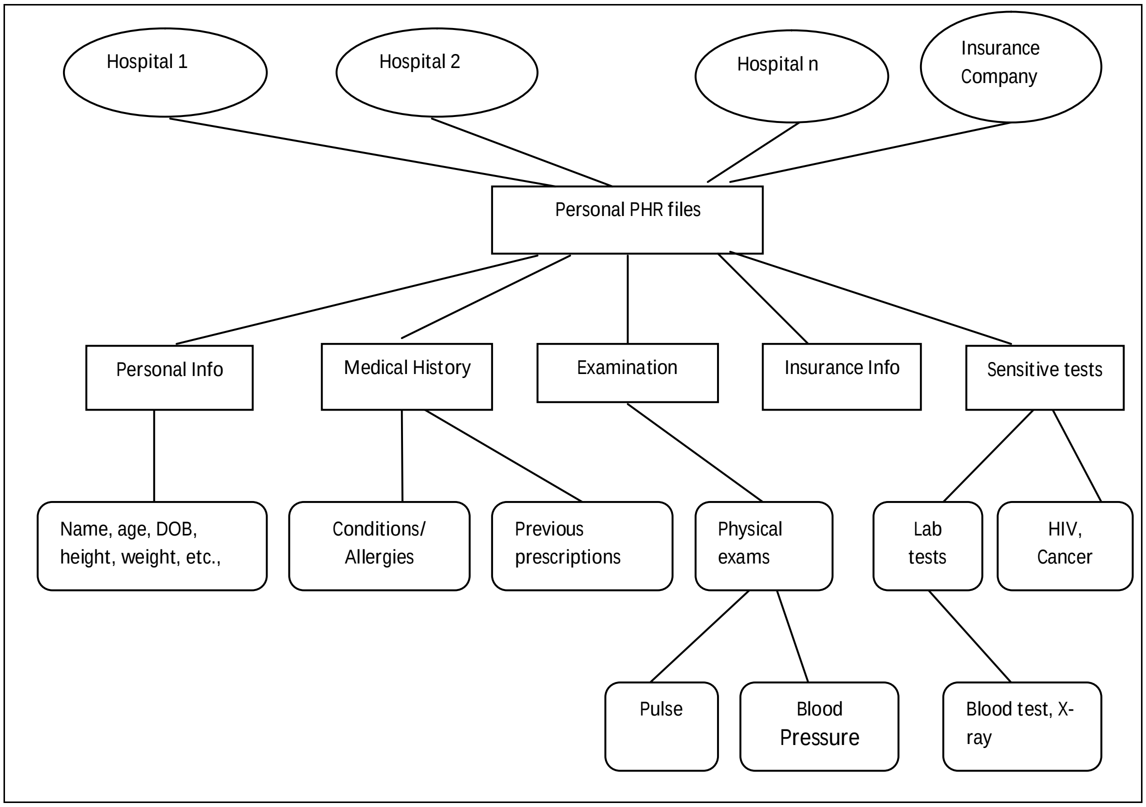


Fig 1: overall example structure of hospital management collaborate with different organization

However some of the advantages over KP-ABE are:

- Multi-organization global resource sharing will handle
- AES encryption used for encryption and decryption more secure that other algorithm
- Owner don't want to stay in online always

IV. PROPOSED FRAMEWORKS

4.1 ACCESS KEY GENERATION

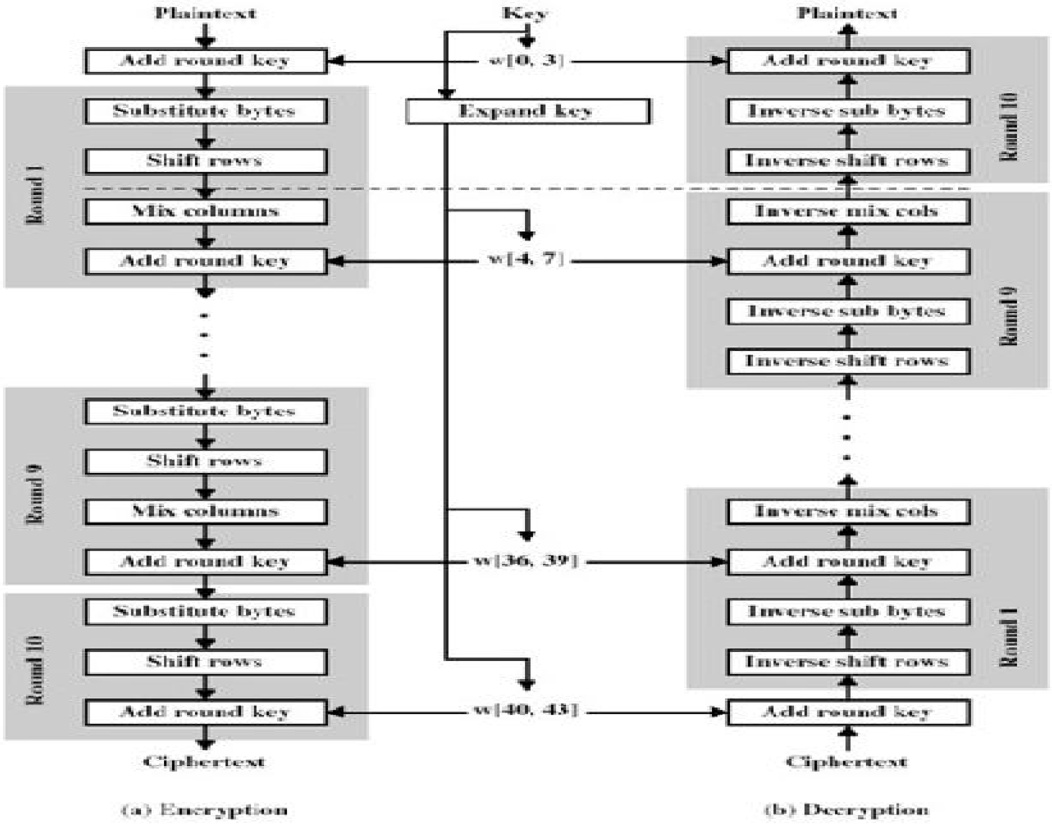
In this module it creates the fine-grained access control key for every user type. The organization admin select the user type and attribute allocation for that user. After select the attributes this module creates the key for access control key. The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

4.2 AES ALGORITHM

AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.



(a) Encryption (b) Decryption

Fig 2: Structure of AES encryption and decryption

The number of cycles of repetition is as follows:

- 10 cycles of repetition for 128 bit keys.
- 12 cycles of repetition for 192 bit keys.
- 14 cycles of repetition for 256 bit keys.

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

4.2.1 High-level description of the algorithm

1. Key Expansion: round keys are derived from the cipher key schedule
2. Initial Round
    1. Add Round Key: each byte of the state is combined with the round key using bitwise xor
3. Rounds

1. Sub Bytes: a non-linear substitution step where each byte is replaced with another according to a lookup table. i.e., $S(a_{i,j}) \ominus a_{i,j} \neq 0xFF$

2. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps. $\mathbf{row}_{(c-n) \bmod 4} \leftarrow \mathbf{t}_c$

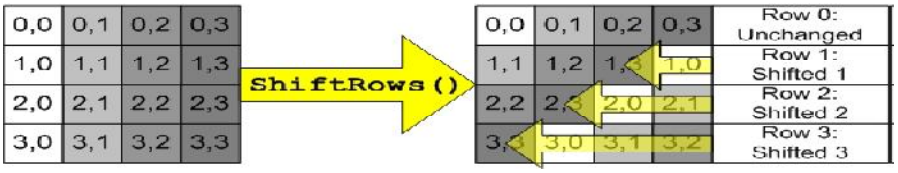


Fig 3: Sample Shift Rows

3. MixColumns: a mixing operation which operates on the columns of the state, combining the four bytes in each column.

$$\mathbf{col}_0 \leftarrow (0x02) \bullet \mathbf{t}_0 \oplus (0x03 \bullet \mathbf{t}_1) \oplus \mathbf{t}_2 \oplus \mathbf{t}_3$$

$$\mathbf{col}_1 \leftarrow \mathbf{t}_0 \oplus (0x02) \bullet \mathbf{t}_1 \oplus (0x03) \bullet \mathbf{t}_2 \oplus \mathbf{t}_3$$

$$\mathbf{col}_2 \leftarrow \mathbf{t}_0 \oplus \mathbf{t}_1 \oplus (0x02) \bullet \mathbf{t}_2 \oplus (0x03) \bullet \mathbf{t}_3$$

$$\mathbf{col}_3 \leftarrow (0x03 \bullet \mathbf{t}_0) \oplus \mathbf{t}_1 \oplus \mathbf{t}_2 \oplus (0x02) \bullet \mathbf{t}_3$$

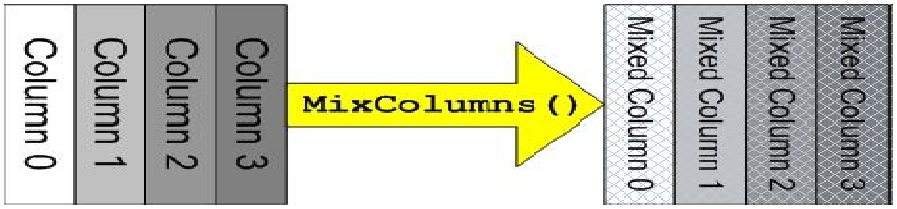


Fig 4: Sample Mix Columns

4. Add Round Key: The actual 'encryption' is performed in the AddRoundKey() function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a expansion schedule. $\mathbf{s}_c \leftarrow \mathbf{s}_c \oplus \mathbf{w}_{\mathrm{round}\,+\,4c}$

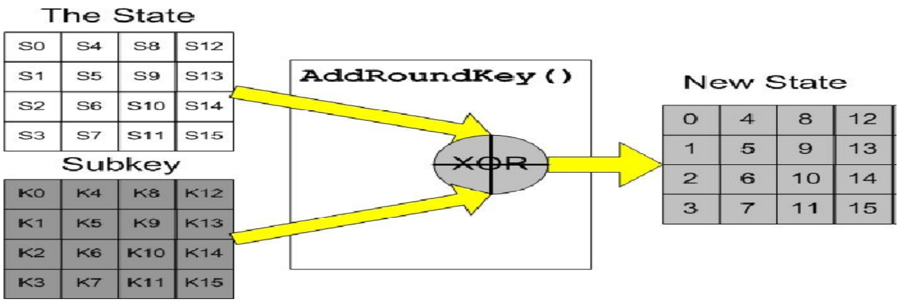


Fig 5: Sample Add Round Keys

4. Final Round (no MixColumns)
    1. SubBytes
    2. ShiftRows
    3. AddRoundKey

The AES algorithms are simple that they can be easily implemented using cheap processors and a minimum amount of memory**.**

4.2.2 Security:

1. **Brute-Force Attack**
   AES is definitely more secure than DES due to the larger-size key.
2. **Statistical Attacks**
   Numerous tests have failed to do statistical analysis of the ciphertext.

3. **Differential and Linear Attacks**
   There are no differential and linear attacks on AES as yet.
4. **Statistical Attacks**
   Numerous tests have failed to do statistical analysis of the ciphertext.

V. CONCLUSION

In this paper, 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 that the only action that is permitted on the local sources is the *read* action. Access control models have been the focus of recent research, including approaches in which the access control model is expressed in terms of tuples that specify who can access which schema element, what type of access is allowed, and how the access rights propagate on the tree.

REFERENCES

[1] C. Dong, G. Russello , and N. Dulay, " Shared and Searchable Encrypted Data for Untrusted Servers," Computer Security, vol.19, pp. 367 -397, 2010.

[2] Ming Li, Shucheng Yu, Yao Zheng ,and ui Ren "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption, " IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

[3] M. Li, S. Yu, N . Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing, " Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] 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," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept.2010.

[5] S.Yu , C. Wang, K. Ren, and W. Lou, " Achieving Secure, Scalable, and Fine Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.