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 RECORD SHARING IN CLOUD COMPUTING USING ATTRIBUTE-BASED ENCRYPTION

Mr. T. Krishnakumar[1], Ms. S. Kayalvili M.E., [2]

Department of CSE, Velalar College of Engineering & Technology, Erode[1]

Assistant Prof, Department of CSE, Velalar College of Engineering & Technology, Erode[2]

**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 employing attribute-based encryption (ABE) have been proposed for access control of outsourced data in cloud computing; however, most of them suffer from inflexibility in implementing complex access control policies. This system not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control. This method used to access the single dataset or local dataset from the cloud computer. Data interoperation systems integrate information from different local sources to enable communication and exchange of data between them. A common model for these systems involves a global representation of the local data, which acts as a mediator for translating queries and conveying data to and from these sources using the global-as view (GAV) approach. In addition, global resource employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. The security of global resource based on security of the cipher text-policy attribute-based encryption (CP-ABE) scheme is proved and its performance and computational complexity is to be analyzed.

## I. INTRODUCTION

Personal Health Record (PHR) is emerged as a patient-centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data center. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to third-party service providers, for example, Microsoft Health Vault, Google Health. While it is exciting to have convenient PHR data 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. Although there exist health care regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities.

Personal health record is the record of a patient who can share her medical information with a large number of users. PHR provide the service for the patients to create and manage their records via web. The PHR service outsourced the records to the cloud servers due to the difficulties in cost of building and maintaining the data. The cloud server is an semi-trusted server and hence the PHR owner encrypt the data before outsourcing.

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

## II. RELATED WORK

Cryptographically enforced access control for outsourced data and attribute based encryption. To realize fine-grained access control, the traditional public key encryption (PKE)-based schemes 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 ABE can be used. Data are encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient. A fundamental property of ABE is preventing against user collusion.

Key-Policy Attribute-Based Encryption (KP-ABE): KP-ABE is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet.

Cipher text Policy Attribute based Encryption (CP-ABE): CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential.

Multi-Authority Attribute-Based Encryption (MA-ABE): MA-ABE method allows any polynomial number of independent authorities to monitor attributes and distribute secret keys.

## III. CONTRIBUTIONS IN THIS PAPER

The attribute based encryption for secure sharing of PHR in cloud computing. For the key management complexity, I divide the users into personal and professional users. Hence the owner needs to manage the keys for small number of users in his/her personal domain and the majority professional users are managed by attribute authorities (AA). The owner and the user both require the minimal key management only. The multi-authority ABE (MA-ABE) in the public domain to avoid the key escrow problem in the central authority.

ATTRIBUTE BASED ENCRYPTION

Using attribute based encryption technique are providing security to the database. A sensitive data is shared and stored on cloud server, there will be a need to encrypt data stored at third party. In Attribute based encryption cipher text labeled with set of attribute. Private key associated with access structure that control which cipher text a user is able to decrypt. I am using 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 the 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-retrieval to solve, and remain largely open up-to-date.
MODULES

USER INTERFACE DESIGN

The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic design may be utilized to support its usability.

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

CLOUD PROVIDER

Cloud Storage is a model of networked computer data storage where data is stored on multiple virtual servers, generally hosted by third parties, rather than being hosted on dedicated servers. Hosting companies operate large data centers; and people who require their data to be hosted buy or lease storage capacity from them and use it for their storage needs. The data center operators, in the background, virtualized the resources according to the requirements of the customer and expose them as virtual servers, which the customers can themselves manage. Physically, the resource may span across multiple servers.

USER ACCESS POLICY

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and 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.

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.

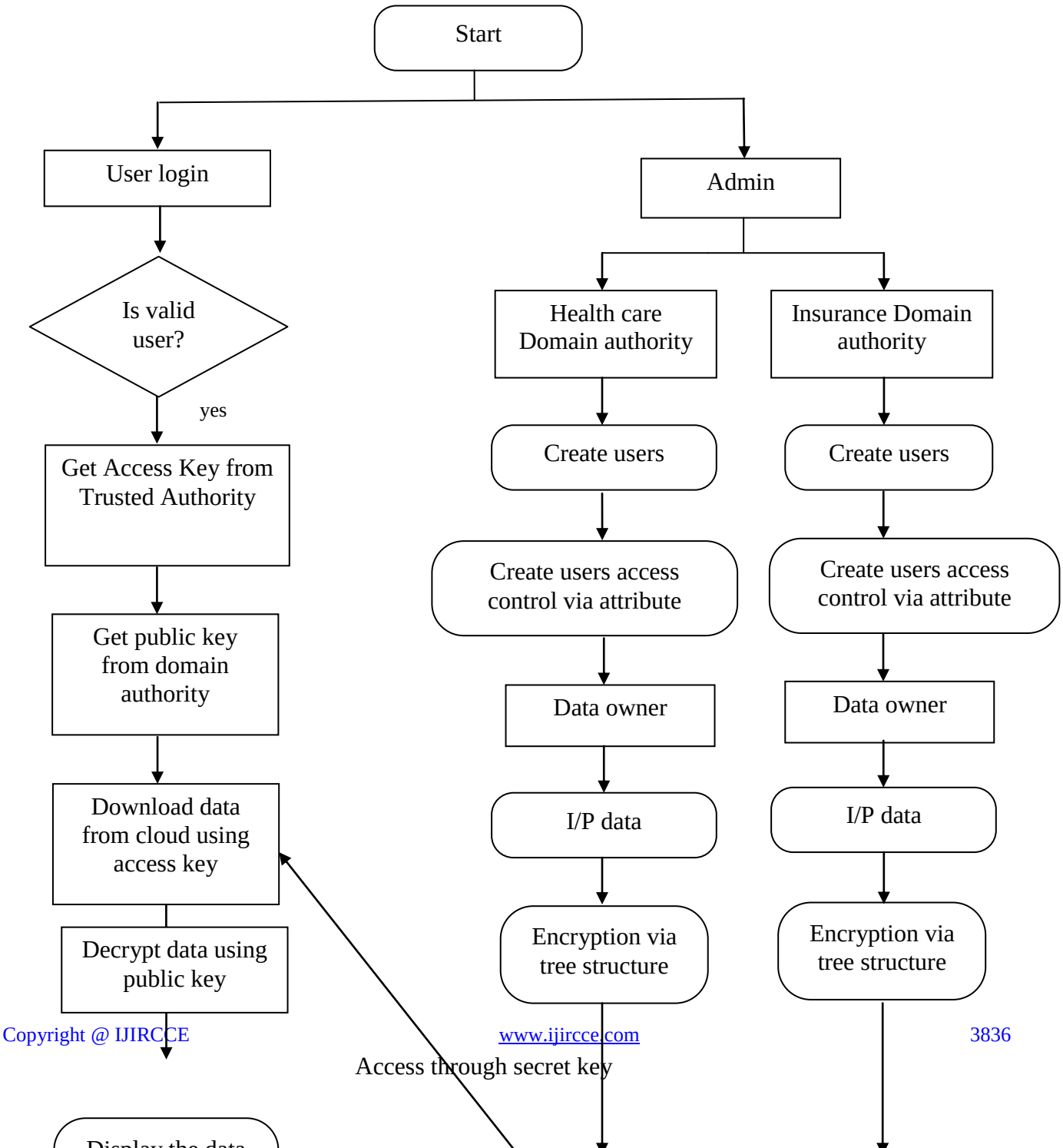
AES ALGORITHM

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.

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

## IV. SYSTEM FLOW DIAGRAM



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

## V.CONCLUSION

The framework addresses the unique challenges brought by multiple PHR owners and users, reduce the complexity of key management while enhance the privacy guarantees compared with previous works. 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, enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, solution is both scalable and efficient.

## REFERENCES

1. Akinyele .A, Lehmann C.U, Green M.D, Pagano M.W, Peterson Z.N.J, and Rubin A.D. (2010) 'Self-protecting electronic medical records using attribute-based encryption on mobile device', Technical report, Cryptology ePrint Archive, http://eprint. iacr.org/2010/565.

2. Benaloh .J, Chase .M, Horvitz .E, and Lauter .K. (CCSW '09) 'Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records' , Proc. ACM Workshop Cloud Computing Security, pp. 103-114, 2009.

3. Dong .C, Russello .G, and Dulay .N. (2010) 'Shared and Searchable Encrypted Data for Untrusted Servers', J. Computer Security, vol. 19, pp. 367-397.

4. Ibraimi .L, Petkovic .M, Nikova .S, Hartel .P, and Jonker .W. (2009) 'Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attribute'.

5. Narayan .S, Gagn´e .M, and Safavi-Naini .R. (2010) 'Privacy preserving EHR system using attribute-based infrastructure', ser. CCSW '10, pp. 47–52