International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:13, No:2, 2019

A Combined Cipher Text Policy Attribute-Based Encryption and Timed-Release Encryption Method for Securing Medical Data in Cloud

G. Shruthi, Purohit Shrinivasacharya

***Abstract*—**The biggest problem in cloud is securing an outsourcing data. A cloud environment cannot be considered to be trusted. It becomes more challenging when outsourced data sources are managed by multiple outsourcers with different access rights. Several methods have been proposed to protect data confidentiality against the cloud service provider to support fine-grained data access control. We propose a method with combined Cipher Text Policy Attribute-based Encryption **(**CP-ABE) and Timed-release encryption **(**TRE) secure method to control medical data storage in public cloud.

***Keywords*—**Attribute, encryption, security, trapdoor.

I. Introduction

CLOUD computing is an information technology that enables access to ubiquitous resources and services over an Internet. [1] A large number of services on infrastructure, platform and software have been developed by different providers. Remote services are ensured to use with a user's data, software and computation. With the strong security mechanism, remote data still face network attacks hardware failures and errors. To ensure correctness and securing a outsourced data becomes a challenging task in cloud computing

II. Working of Cloud

Cloud computing is a technology also termed as demand computing that provides processing of shared resources to computers and other devices on demand. These shared resources can be provisioned with least minimal effort such as networks, applications, storage and services. Cloud computing and storage solutions provide enterprises and users with several capabilities to store and process data in third party data centers.

III. Proposed System

Hong et al. [1] used a combined scheme of CP-ABE and TRE. In our system same approaches are used with additional capabilities for securing our medical data.

In the proposed system, patient data are secured with time factor with the help of the methods TRE and CP-ABE [10], practical methods are applied on medical data to get effective access with minimum difficulty to cipher policy text attribute encryption scheme.

Shruthi G. is Research scholar, Siddaganga Institute of Technology, Tumakuru, India (phone: 9739049892, e-mail: shruthiindbit@gmail.com).

Dr. Purohit Shrinivasacharya is Associate Professor, Dept of ISE, Siddaganga Institute of Technology, Tumakuru, India (e-mail: purohitsn@gmail.com).

IV. Advantages of Proposed System

1) Medical data are secured from illegal access.
2) Risk of Trusted CA is reduced.
3) Risk of owners and users is reduced.
4) Patient data are secured by time seal.
5) Registered authenticated users are allowed to view the patient data within the time seal.
6) Users can search the patient file using the keywords. He can download the file by using the secret key.
7) Only the doctor can view and edit the file but the others and insurance company allowed only viewing the patient file without any modifications.
8) Secret key is generated only to the registered user and owners by AES algorithm

V. Literature Survey

Li and Yu [11] have used combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption.

Qin et al. [3] gave a solid and inspiring survey of proxy re-encryption from different perspectives to offer a better understanding of this primitive. They have reviewed the state-of-the-art of the proxy re-encryption by investigating the design philosophy, examining the security models and comparing the efficiency and security proofs of existing schemes.

Ren et al. [5] explain different prominent challenges on security and motivate further findings of security solutions for a trusted public cloud environment

Yang et al. [6] propose data access control for multi authority cloud storage (DAC-MACS), provide a secure data access control scheme with decryption and revocation. A new CP-ABE scheme called multi authority with decryption, and attribute suppression method was introduced with both forward security and backward security for weaker security assumptions.

VII. System Design

Data owner, search user, cloud service provider (ADMIN) and central authority are the four modules developed in the system design. Below is the description of each module provided.

In data owner module, there are p numbers of data owner are present. Owner should register themselves before performing any operations with user name and password. Next is the Data Owner, who can access the file, upload the file and can do security check on the same file and if it is successful it will be sent to the server. Following are the functions of the data owner: registration, file upload, file view, unset/set the time factor, searching a particular user or user data with a keywords with p numbers of users present. User should register before doing some operations, and registered user details are stored in user module. After successful registration he has to login by using authorized user name and password. With successful login he will do the following operations, like, search a particular query, requesting for secret key, accessing the files etc.

Cloud server provider can perform functionalities such as he can view file information and he/she can activate user (doctor) and owner (patients).

In the cloud environment, cloud administrator manages multiple attribute authority, and attribute authority manages both issuing of file attributes and user. We developed the following functionalities for the cloud administrator: Login Information, User Information, Issuing Secret Key.

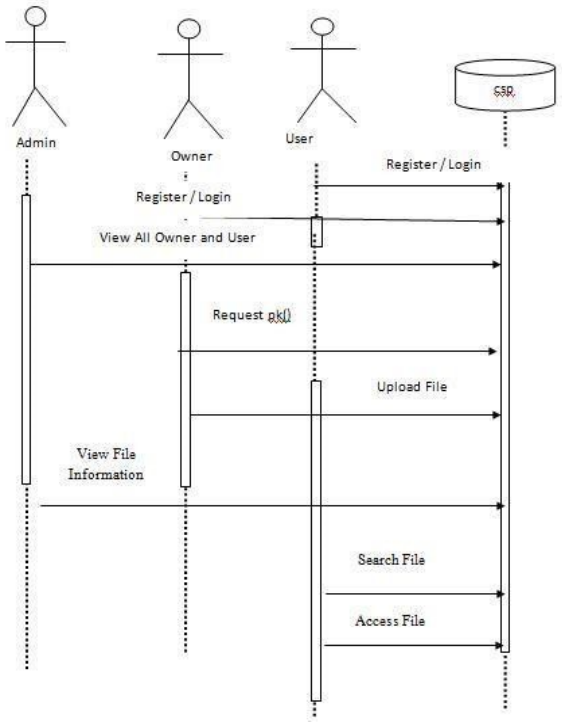

Fig. 1 Different Roles in System Design

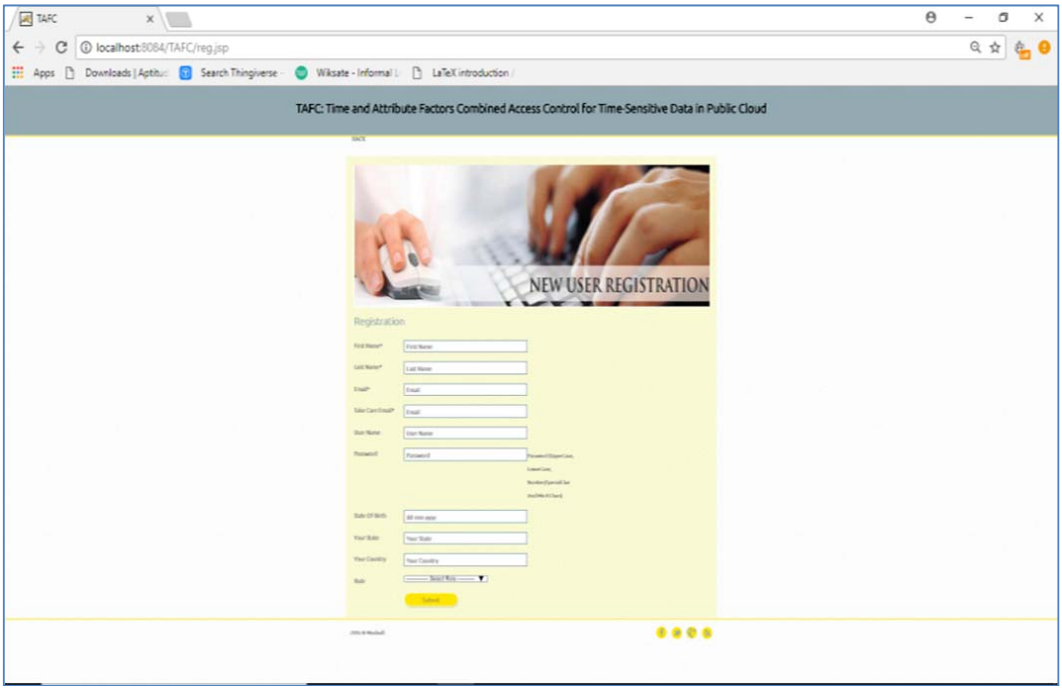

Fig. 2 Owner Registration page

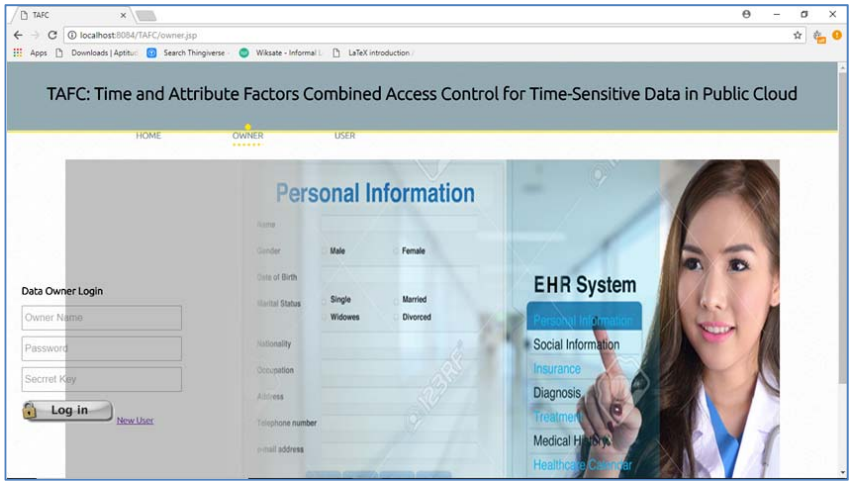

Fig. 3 Login page

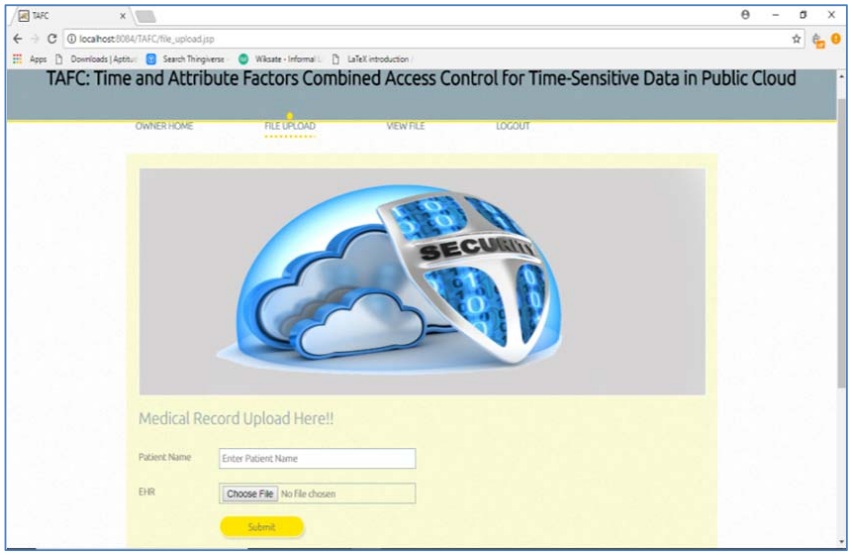

Fig. 4 Uploading a File

Fig. 5 Viewing File

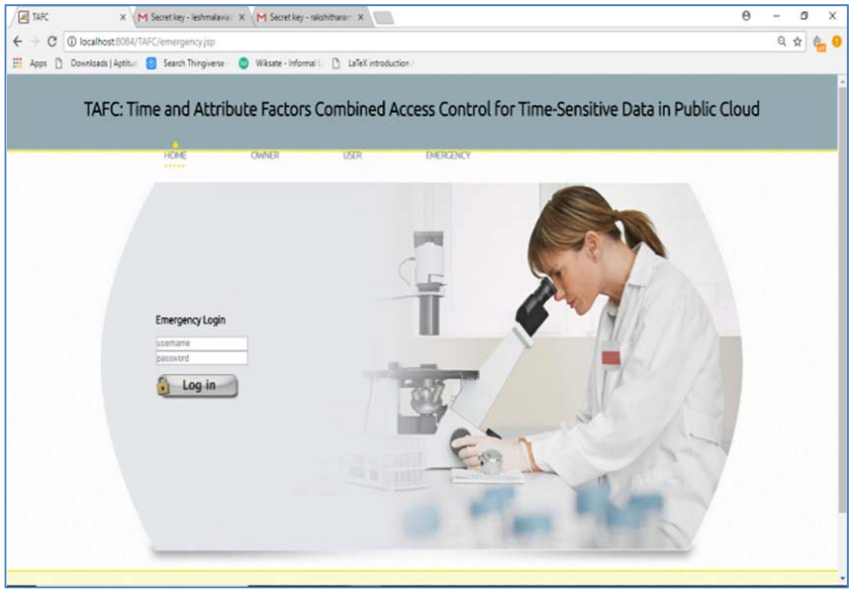

Fig. 6 Emergency Login

Fig. 7 Granting Time Seal for Users

VIII. System Security

The following are the prototypes and encryptions used:

A. CP-ABE [1], [7]

In this prototype, a set of attributes is tied with user private key to decrypt the encrypted message. Data can be accessed if only and if the attribute satisfies the access policy.

The following two polices were used in our scheme [3], [4]: CP-ABE and Advanced Encryption Standard (AES) which uses Trapdoor mechanism and TRE.

B. AES [2]

AES is a simple data protection encryption model used in cloud which contains massively scalable data, which ensures, confidentiality and data security. AES uses a block length of 128 with different k length. We are encrypting using 128 bit k lengths. Minimum 10 rounds of encryption are carried out for processing of 128 bit keys. Memory and time consumption is less in AES compared to other Encryption methods to provide data security.

C. TRE [1], [9], [10]

TRE is combined into CP-ABE, to get an appropriate secure

measure for cloud storage. We had taken time as an attribute with number of keys used as a secure parameter for all users to access a patient data, so that only one key related to time factor is issued by cloud admin.

IX. Results

In this system design we will consider that owner is the patient and the users are doctor, patient guardian and insurance company. The owner i.e. patient should register himself then only he/she will be able to login for further operations. [8] Once the patients register successfully, central authority will sent a secret key to the patient mail, then he/she can login with the same key provided in the mail id. Once the patients login he/she can upload his medical related files such as scanning report, blood report etc.; these files are uploaded to the cloud.

Registration procedure applies to patient guardian and insurance company with different user privileges.

Next the doctor can perform the view operation of patient data. In the owner page time seal is used to give access permission for the doctor to access the patient file The doctor can access the file within the time given by the patient. As soon as time seal starts doctor can search the patient file by using the keywords, he can download the file by using the secret key which is already in his mail sent during registration process.

The doctor can view and edit the file but the nurse and insurance company can only view the file. The emergency department requests the patient file from caretaker/guardian when the patient is in unconscious stage. When the caretaker/ guardian activates the permission, the emergency department will download the file to view the patient details. Any modification is not allowed here.

Figs. 2-8 show some of the views of our owner login and file operations which are implemented using java as frontend and MySQL as backend.

Fig. 8 Downloading patient data

X. Conclusion

Our work proves that our scheme can protect the unpublicized time sensible patient data, only the authorized user can view the patient data within a given time seal with less burden to CA and data owners. If the patient is in unconscious state, data access privilege has to be granted to emergency guardian as a Future Enhancement

References

[1] "Jianan Hong, Weikeng Chen, David S. L. Wei and Nenghai Yu, "TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud", IEEE Transactions on Services Computing, IEEE, 2017.

[2] Huijun Zhu, Licheng Wang and Haseed Ahmad, "Key policy attribute-based encryption with equality test in cloud computing", IEEE Access, 2017

[3] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing", IEEE Transactions on Services Computing, 2016.

[4] F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef, "Transparent data deduplication in the cloud", in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,pp.886– 900,ACM, 2015.

[5] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud", IEEE Internet Computing, Vol. 16, pp. 69–73, 2012.

[6] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DACMACS: Effective data access control for multi-authority cloud storage systems", IEEE Transactions on Information Forensics and Security, Vol. 8, pp.1790–1801, 2013.

[7] Q. Liu, G. Wang, and J. Wu, "Time-based proxy reencryption scheme for secure data sharing in a cloud environment", Information Sciences, Vol. 258,pp. 355–370, 2014.

[8] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable-encryption in unreliable clouds", in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM '11), pp. 1–5, IEEE, 2011.

[9] J. Li, W. Yao, Y. Zhang, and H. Qian, "Flexible and fine grained attribute-based data storage in cloud computing", IEEE Transactions on Services Computing, Available online, 2016.

[10] X. Zhu, S. Shi, J. Sun, and S. Jiang, "Privacy-preserving attribute- based ring sign encryption for health social network", in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM '14), pp. 3032–3036, IEEE, 2014

[11] L. Xu, F. Zhang, and S. Tang, "Timed-release oblivious transfer", Security and Communication Networks, Vol. 7, pp. 1138–1149,2014.