Time & Attribute based Encryption-Decryption Scheme

Amrutha V[1] Gayathri S R[2] Gaurav[3] Kashish Kumar[4] Pushpaveni H P[5]
[5]Assistant Professor
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]Dr. Ambedkar Institute of Technology (Bengaluru), India

Abstract— The new paradigm of outsourcing knowledge to the cloud could be an ambiguous sword. On one hand, it frees knowledge homeowners from the technical management, and is less complicated for knowledge homeowners to share their knowledge with intended users. On another hand, it poses new challenges on privacy and security protection. To shield knowledge confidentiality against the honest-but- curious cloud service supplier, various works are proposed to support fine-grained knowledge access management. However, till now, no schemes will support each fine-grained access management and time-sensitive knowledge business. In this paper, by embedding timed-release encryption into CP-ABE (Ciphertext-Policy Attribute-based Encryption)[1], we are proposing a replacement naming Time and Attribute based Encryption-Decryption Scheme in Cloud Computing (TAEDS).

Key words: TAEDS (Time and Attributes based Encryption-Decryption Scheme), NetBeans, MySQL, CP-ABE, Trapdoor

I. INTRODUCTION

The existing system cannot work up to one's expectations. There are several security issues like forward and backward security and CP-ABE being unable to support gradual access privilege.

To overcome this issue, we propose an efficient Time and Attribute based Encryption-Decryption Scheme (TAEDS) for time-sensitive data in public cloud. Our scheme possesses two important capabilities:

1) It inherits the property of fine granularity from CP-ABE;
2) By introducing the trapdoor mechanism, it further retains the feature of timed release from TRE. Note that in TAFC, the introduced trapdoor mechanism is only related to the time factor, and only one corresponding secret needs to be published when exposing the related trapdoors. This makes our scheme highly efficient, which only brings about little overhead to the original CP-ABE based scheme.

The proposed system provides certain benefits:

Ciphertext-policy attribute-based encryption (CP-ABE) is a useful cryptographic method for data access control in cloud storage. All these CP-ABE based schemes enable data owners to realize fine-grained and flexible access control on their own data. On contrary, CP-ABE takes care of users' access privilege based on their inherent attributes only without considering factors which might be critical, such as the time factor. The time factor usually plays an important role in dealing with time-sensitive data (e.g. to publish a latest e-magazine, or expose an organization's future business plan). In these scenarios, both the mechanism of access privilege timed releasing and fine-grained access control should be together taken into consideration.

On combining CP-ABE with TRE in public cloud storage, we put forward an effective way to know secure fine-grained access control for time-sensitive data. In the proposed scheme, the data owner can autonomously assign intended users and their respective access privilege releasing time slots. Besides realizing the function, it is proved that the negligible burden is upon owners, users and the trusted CA.

A rigorous security proof is given to validate that the proposed scheme is secure and effective

II. BLOCK DIAGRAM

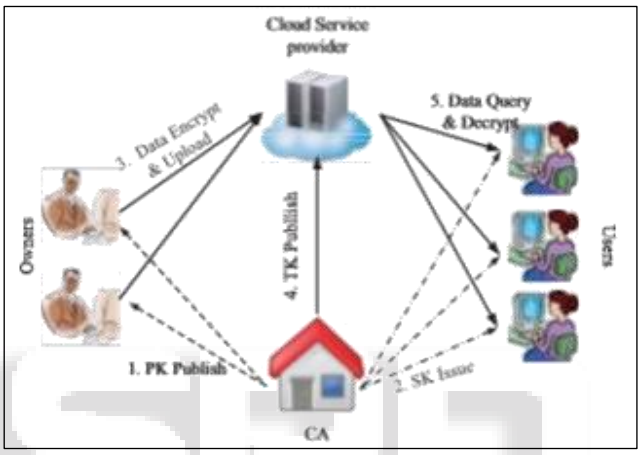

Fig. 2.1: Block Diagram for TAEDS

III. WORKING

To properly elaborate the concept of TAEDS, we have implemented it in a client and server platform. Initiation of the procedure starts from the data owner or owner (patient) registering on the portal using his/her mail id. As soon as owner registers, a secret key is generated and sent through mail which is registered and used for login. Upon logging in, owner uploads the necessary documents to cloud. The owner will have access to his/her uploaded documents. After uploading, the owner can set a time seal. The time seal allows the recipient to access the specific document within that time span. And on addition to it, the files can be accessed only with the secret key.

After completion of owner part, the user will register when he/she is notified. As soon as user registers, the secret key is generated and sent through mail which was used for login. Then user will search for the owner by entering keywords as per directed and a send a request to owner for accessing the file. After receiving the request, owner activates the request and the user can download a file using secret key and only the doctor/user can update or download the files.

In addition to this takecare is used which act as alternative to user. An emergency can be filed on behalf of data owner and they send a file request to takecare. The takecare activates the request and thus emergency can download the file using secret key. On other hand admin will have all information about user, owner and downloaded files.

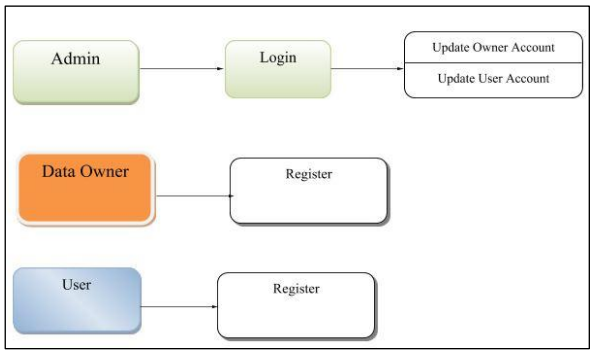

Fig.3.1 Level 0

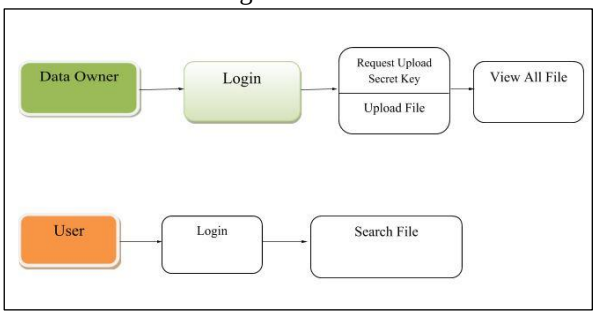

Fig. 3.2: Level 1

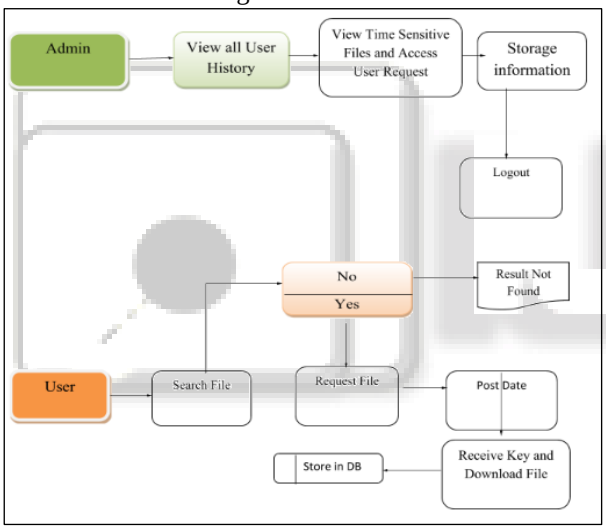

Fig. 3.3: Level 2

IV. SOFTWARE SPECIFICATIONS

A. JAVA/J2EE

Enterprise Edition (Java EE) of Java platform is the standard in community-driven enterprise software. Java EE is acquired using the Java Community Process, with contributions from commercial and open source organizations, industry experts, Java User Groups, and infinite number of individuals. Each release adds new features that matches with industry needs, improves application adaptability, and increases developer productivity.

Today, Java EE offers a rich enterprise software platform and more than 20 compliant Java EE implementations to choose from.

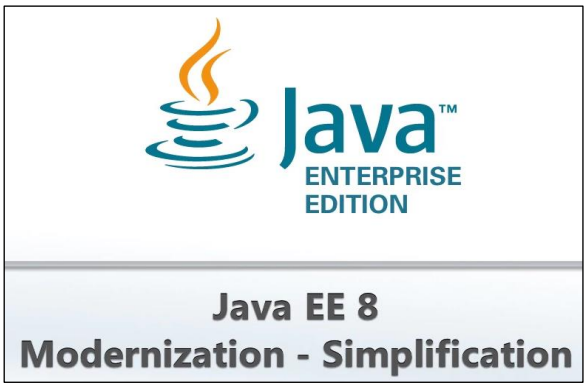

Fig. 4.1: Java/J2EE

B. NETBEANS 7.2.1

The NetBeans IDE is an integrated development environment available for Mac, Linux, Windows, and Solaris. The NetBeans project comprises of an open-source IDE and an application platform that allows developers to create web, desktop, enterprise, and mobile applications using the Java platform, as well as JavaScript, Ajax, PHP, and C/C++.

The NetBeans project is backed up by an extra-ordinary developer community and offers substantial documentation and training resources as well as a sundry selection of third-party plugin software [5].

Fig. 4.2: NetBeans

C. MySQL

MySQL is an all-accessible relational database management system (RDBMS). The MySQL development project has made its source code accessible under the conditions of the GNU General Public License, as well as under diverse proprietary agreements. Ownership and sponsorship of MySQL is carried out by a single for-profit organization, the Swedish company MySQL AB. It now owned by Oracle Corporation. For proprietary use, numerous paid editions are available, and offer additional features.

Fig. 4.3: MySQL

V. RESULTS

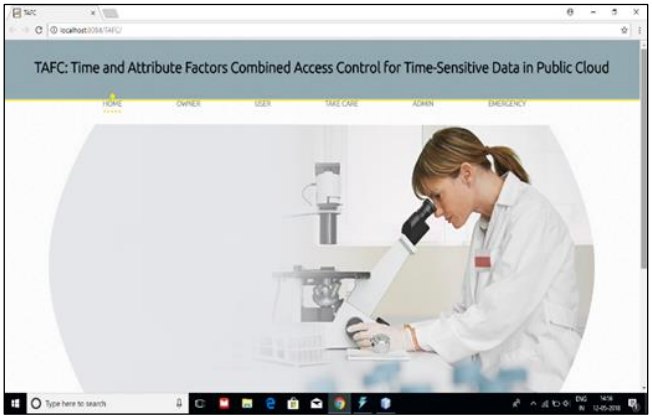

Fig. 5.1: Menu page for TAEDS

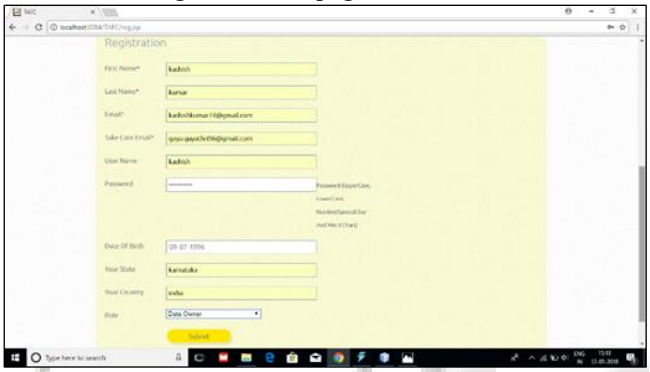

Fig. 5.2: Information feed page for TAEDS

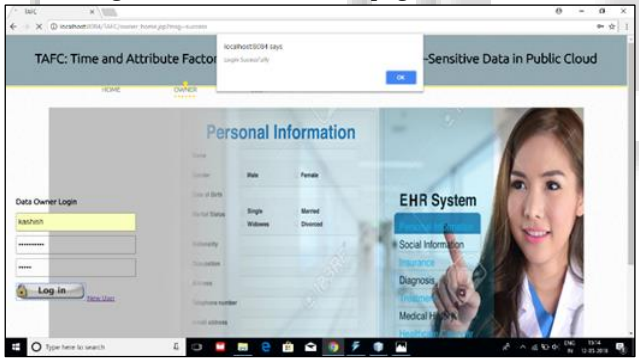

Fig. 5.3: Login Successful

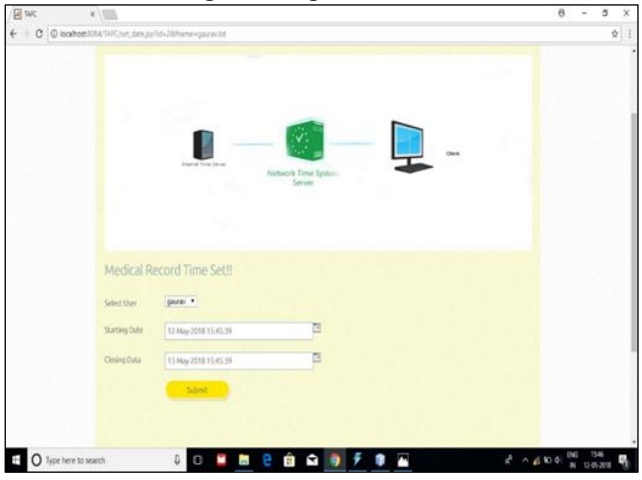

Fig. 5.4: Setting Time Constraint

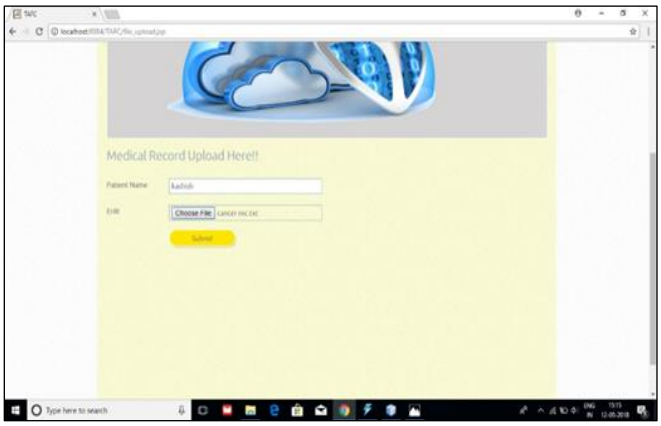

Fig. 5.5: Uploading File to Cloud

VI. ADVANTAGES

- On combining CP-ABE with TRE in public cloud storage, we put forward an effective way to know secure fine- grained access control for time-sensitive data. In the proposed scheme, the data owner can autonomously assign intended users and their respective access privilege releasing time slots. Besides realizing the function, it is proved that the negligible burden is upon owners, users and the trusted CA.
- A rigorous security proof is given to validate that the proposed scheme is secure and effective and data is accessible to one having correct access privilege.

VII. CONCLUSION

This paper aims at fine-grained access control for time sensitive data in cloud storage. One challenge is to simultaneously achieve both flexible timed release and fine granularity with lightweight overhead, which was not explored in existing works. In this paper, we proposed a scheme to achieve this goal. Our scheme seamlessly incorporates the concept of timed-release encryption to the architecture of ciphertext policy attribute-based encryption. With a suit of proposed mechanisms, this scheme provides data owners with the capability to flexibly release the access privilege to different users at different time, according to a well-defined access policy over attributes and release time. We further analyzed access policy design for all probable access requirements of time sensitive, through appropriate placing of time trapdoors. The analysis shows that our idea can preserve the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners. It thus well suits the practical large-scale access control system for cloud storage.

This mainly focuses on secure storage of data in public cloud. It also provides facility for grain grained access control of time sensitive data. To achieve this by integrating CP-ABE and TRE mechanism. Based on this scheme the data owners can decide which user able to access data and provide relevant access privilege releasing time points according to a well-defined access policy over attribute and releasing time. And it provides a lightweight overhead on both central authority and data owners. This mechanism is highly applicable for large scale access control system for cloud storage.

ACKNOWLEDGMENT

This research was permitted and encouraged by our Institution, Dr. Ambedkar Institute of Technology. We thank all the people responsible for the same.

We further thank our HOD, Dr. Siddaraju, who provided insight that greatly assisted the research.

We would also like to show our gratitude to our respective families for their constant show of affection and care during the research period.

REFERENCES

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

[2] 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.

[3] R. Masood, M. A. Shibli, Y. Ghazi, A. Kanwal, and A. Ali, "Cloud authorization: exploring techniques and approach towards effective access control framework," Frontiers of Computer Science, vol. 9, no. 2, pp. 297–321, 2015.

[4] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[5] www.oracle.com

