TIME AND CHARACTERISTICS ISSUES COMBINED ACCESS CONTROL FOR TIME SENSITIVE DATA STORAGE IN CLOUD

[1] Dr.P.Chitti Babu, [2] G.Chandana

[1]Professor &Principal , [2]MCA Student
[1,2]MCA Department,
[1,2]Annamacharya PG college of Computer Studies , Rajampet, Y.S.R kadapa, Andhra Pradesh, India

Abstract : The new model of subcontracting data to the cloud is a two-edged sword. On the one hand, it frees data owners from the official management, and is easier for data owners to share their data with proposed users. On the other hand, it brings about new experiments on privacy and security protection. To protect data privacy against the honest-but-curious cloud service provider, numerous works have been proposed to support fine-grained data access control. However, till now, no schemes can support both fine-grained access control and time-sensitive data publishing. In this work, by establishing timed-release encryption into CP-ABE (Cipher-text Policy Attribute-based Encryption). I propose a new time and characteristic issues combined access control on time-sensitive data for cloud storage. Based on the proposed scheme, I further propose an efficient approach to design access policies faced with various access requirements for time-sensitive data. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for time sensitive data storage in public cloud.

Index Terms: Introduction, cloud computing, existing work, proposed work

I. INTRODUCTION

Design an effective architecture to realize our scheme, in which we redesign an entity (the central authority, CA) to be responsible for the timed-release function. Besides distributing attribute-associated private keys, CA only needs to periodically publish universal time-related tokens to release access privileges. Such architecture occupies only a small amount of cost to provide our required access control scheme, which is reasonable and worthy. The main purpose of this application is providing the access control with time and attribute factor for time sensitive data stored in cloud. Providing access control with time and attribute combined factors for sensitive data. It is providing TRE and CP-ABE integration for fine grained access control.

II. EXISTING WORK

To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Cipher text-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques.In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labeled with their own attributes.

limitations

- Use CP-ABE Access privileges based only on attribute factor but not critical factor of time factor.
- These schemes are not secure in access privileges.
- Lack of fine-grained access control.

III. PROPOSED WORK

In this work, proposed an efficient time and attribute factors combined access control scheme, named TAFC, 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 trap door 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 trap doors. This makes our scheme highly efficient, which only brings about little overhead to the original CP-ABE based scheme.

features

- By integrating TRE and CP-ABE in public cloud storage, I propose an efficient scheme to realize secure fine grained access control for time-sensitive data.
- To the best of my knowledge, we are the first to study the approach to design structures for general time-sensitive access requirements.
- Providing time and attribute factor access control.
- More secure against attackers.
- More efficient.

IV. PROPOSED FRAME WORK

- Data Owner
- Cloud Server
- Certificate Authority
- Data Consumer/End User

Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

Cloud Server

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. It is responsible for authorizing all end users.

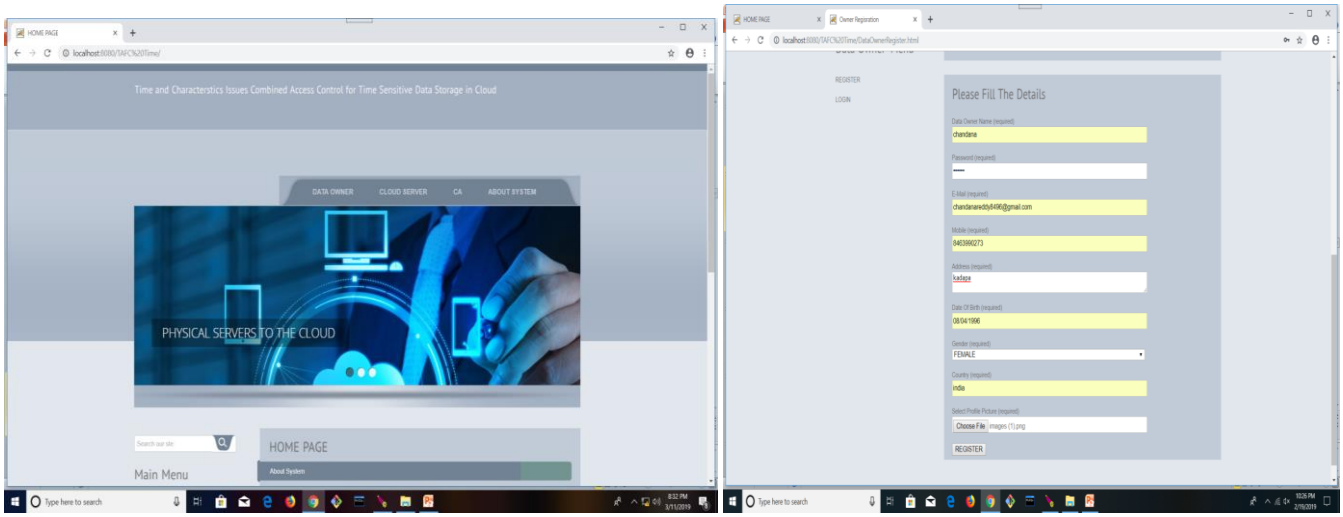
Certificate Authority

CA who is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

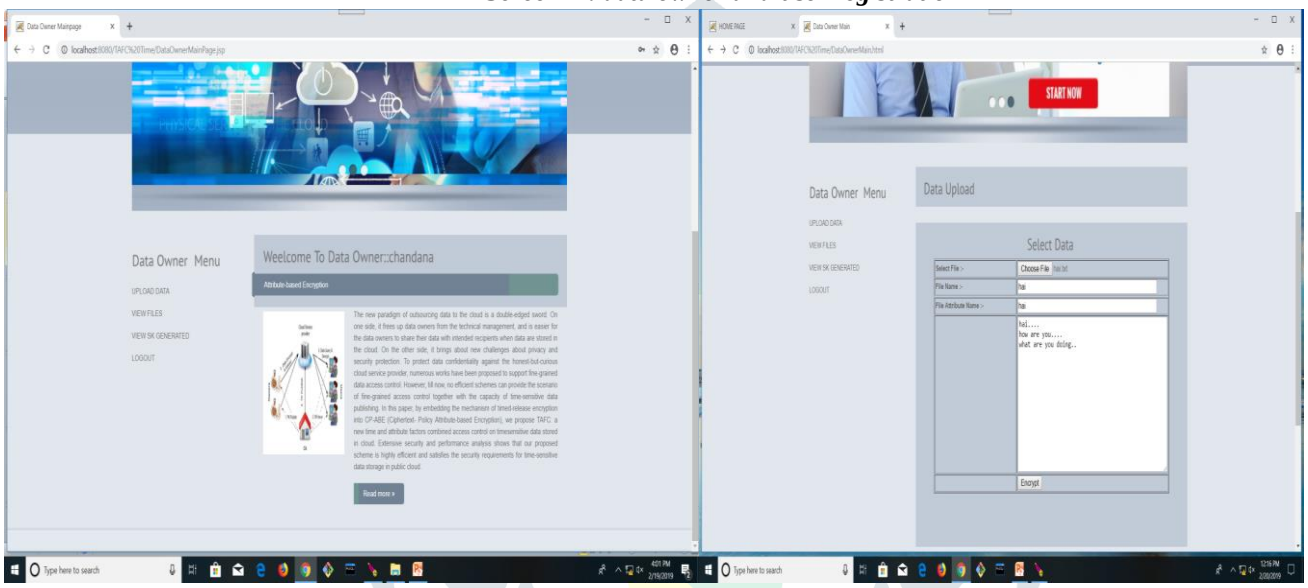
Data Consumer/End User

In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Data owner and the Data users are controlled by the data owner only. Users may try to access data files either within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to CA to generate secret key and CA will generate the key and send to corresponding end user.

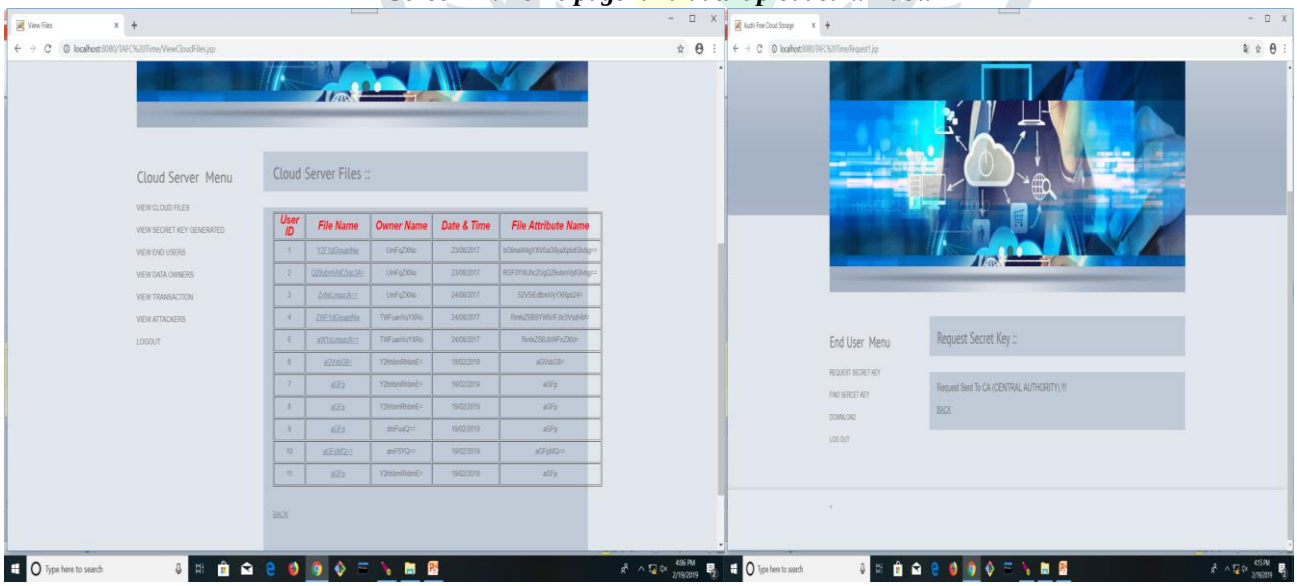
V. RESULTS



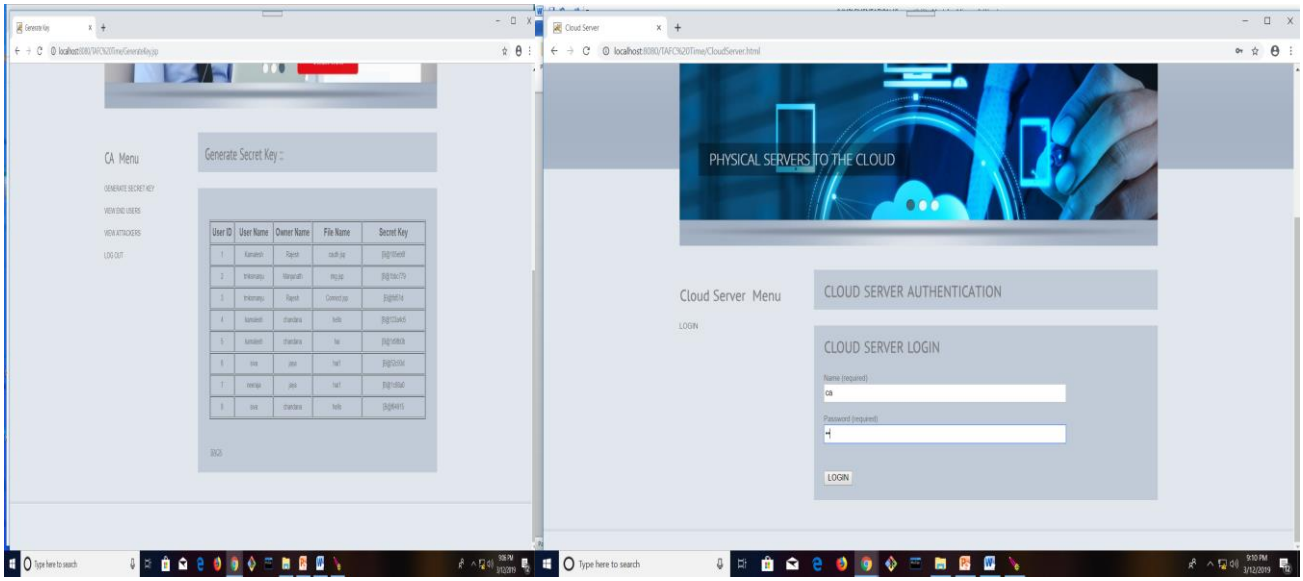
Screen 1 : data owner and user registration



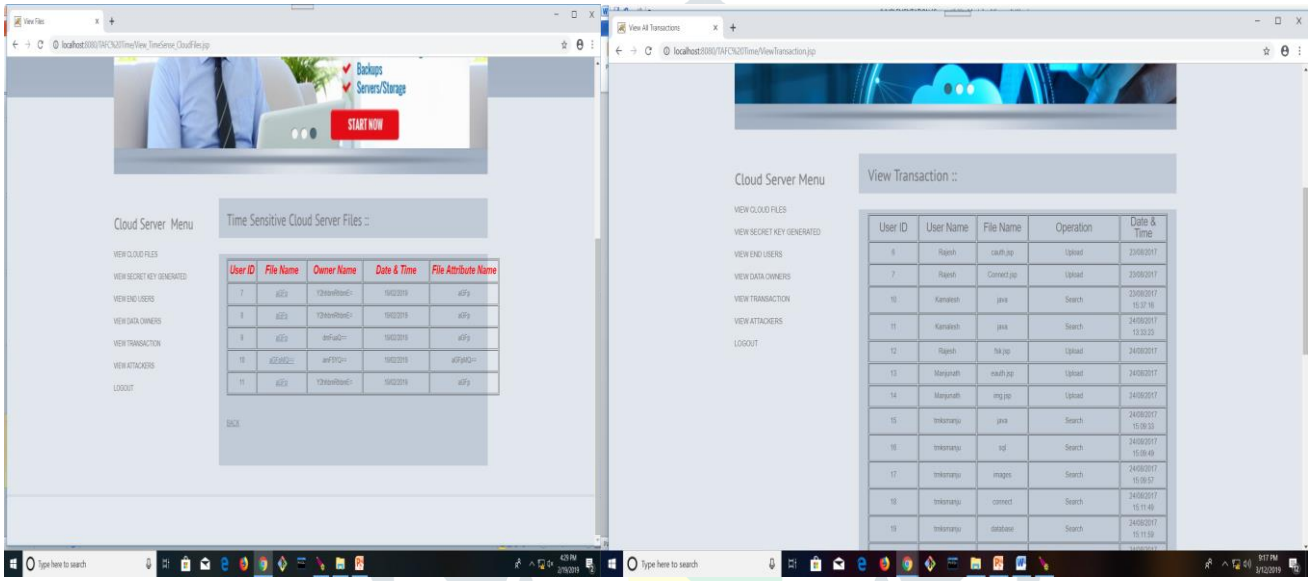
Screen 2 : home page and data uploaded window



Screen 3 data uploaded and request fr secret key



***Screen 4* Generate Secret Key for CA and Cloud Login**



Screen 5 Time Sensitive Cloud Server Files View Transaction Files in Cloud Server

V CONCLUSION AND FUTURE WORK

Finally, I conclude that, at fine-grained access control for time sensitive data in cloud storage. One challenge is to simultaneously achieve flexible timed release and fine granularity with lightweight overhead, which is not provided in related work. I propose a scheme to achieve this goal. My scheme seamlessly incorporates the concept of timed-release encryption to the architecture of cipher text-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. The analysis shows that our scheme can protect the confidentiality of time-sensitive data, with a lightweight overhead on both CA and data owners, thus well suits the practical large-scale access control system for cloud storage.

REFERENCES

[1] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "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, pp. 131–143, 2013.

[4] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, "Privacypreserving granular data retrieval indexes for outsourced cloud data," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 601–606, IEEE, 2014.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM2011), pp. 1–5, IEEE, 2011.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy\ attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007), pp. 321–334, IEEE, 2007.

[7] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001.

[8] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," tech. rep., Massachusetts Institute of Technology, 1996.

[9] K. Yuan, Z. Liu, C. Jia, J. Yang, and S. Lv, "Public key timed-release searchable encryption," in Proceedings of the 2013 Fourth International Emerging Intelligent Data and Web Technologies (EIDWT2013), pp. 241–248, IEEE, 2013.

[10] Q. Liu, G. Wang, and J. Wu, "Time-based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, no. 3, pp. 355–370, 2014.

[11] L. Xu, F. Zhang, and S. Tang, "Timed-release oblivious transfer," Security and Communication Networks, vol. 7, no. 7, pp. 1138– 1149, 2014.

[12] E. Androulaki, C. Soriente, L. Malisa, and S. Capkun, "Enforcing location and time-based access control on cloud-stored data," in Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS2014), pp. 637–648, IEEE, 2014.

[13] C.-I. Fan and S.-Y.Huang, "Timed-release predicate encryption and its extensions in cloud computing," Journal of Internet Technology, vol. 15, no. 3, pp. 413–426, 2014.