International Journal For Technological Research In Engineering
Volume 5, Issue 9, May-2018 *ISSN (Online): 2347 - 4718*

THREE WAY SELF- DESTRUCTING SCHEME IN CLOUD COMPUTING

S.Divya
Department of Computer Science, PG Student, Sri Ramanujar Engineering College, Tamil Nadu, India

ABSTRACT: Cloud computing is considered as the next step in the evolution of on-demand information technology which combines a set of existing and new techniques from research areas such as service-oriented architectures (SOA) and virtualization. With the rapid development of versatile cloud computing technology and services, it is routine for users to leverage cloud storage services to share data with others in a friend circle e.g., Dropbox, GoogleDrive and AliCloud. The shared data in cloud servers, however, usually contains users' sensitive information andneeds to be well protected. As the ownership of the data is separated from the administration of them, the cloud servers may migrate users data to other cloud servers in outsourcing or share them in cloud searching. environment. In order to meet this challenge, it is necessary to design a comprehensive solution to support user-defined authorization period and to provide fine-grained access control during this period. The shared data should be self-destroyed after the user-defined expiration time.

I. INTRODUCTION

In many applications, the data owner wants to share information with several users according to the security policy based on the users' credentials. Attribute based encryption (ABE) has significant advantages based on the tradition public key encryption instead of one-to-one encryption because it achieves flexible one-to-many encryption. data security and fine-grained access control. In the keypolicy ABE (KP-ABE) scheme to be elaborated in this paper, the ciphertext is labeled with set of descriptive attributes. Only when the set of descriptive attributes satisfies the access structure in the key, the user can get the plaintext. In general, the owner has the right to specify that certain sensitive information is only valid for a limited period of time, or should not be released before a particular time.

Timed-release encryption (TRE) provides an interesting encryption service where an encryption key is associated with a predefined release time, and a receiver can only construct the corresponding decryption key in this time instance. On this basis, Paterson et al. proposed a time specific encryption (TSE) scheme, which is able to specify a suitable time interval such that the ciphertext can only be decrypted in this interval (decryption time interval, DTI). Thebids(ciphertext) should be kept secret during the bidding phase (a specific time interval). However, applying the ABE to the shared data will introduce several problems with regard to timespecific constraint and self-destruction, while applying the TSE will introduce problems with regard to fine-grained access control.If the user enter the Incorrect keythree times, the data will be self-destructed. Thus, in this paper, we attempt to solve these problems by using KPABE and adding a constraint of time interval to each attribute in the set of decryption attributes.

II. RELATED WORKS

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information—identity privacy—to public verifiers. We propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Big data, because it can mine new knowledge for economic growth and technical innovation, has recently received considerable attention, and many research efforts have been directed to big data processing due to its high volume, velocity, and variety (referred to as "3V") challenges.

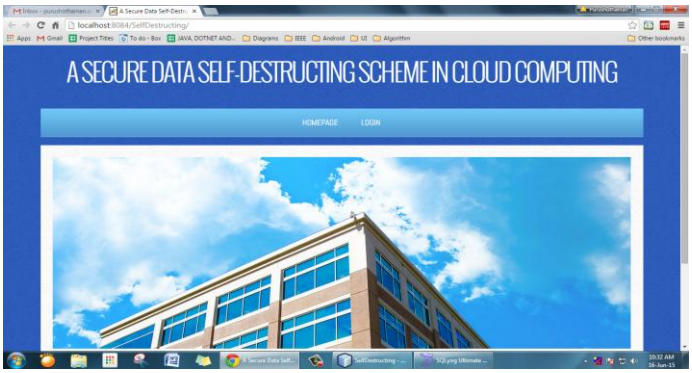
However, in addition to the 3V challenges, the flourishing of big data also hinges on fully understanding and managing newly arising security and privacy challenges. If data are not authentic, new mined knowledge will be unconvincing; while if privacy is not well addressed, people may be reluctant to share their data. Because security has been investigated as a new dimension, "veracity," in big data, in this article, we aim to exploit new challenges of big data in terms of privacy, and devote our attention toward efficient and privacy-preserving computing in the big data era. Specifically, we first formalize the general architecture of big data analytics, identify the corresponding privacy requirements, and introduce an efficient and privacy-preserving cosine similarity computing protocol as an example in response to data mining's efficiency and privacy requirements in the big data era.

III. PROPOSED METHODOLOGY

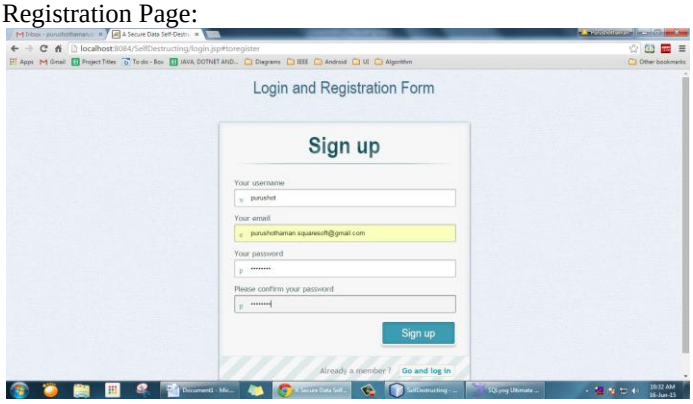
The purpose of the project is to provide more security. when it comes to managing sensitive data the privacy of your cloud-based data is another consideration. In order to tackle this problem, we propose a novel secure data three way self destructing scheme in cloud computing using AES/DES Double Encryption Algorithm. . By using this, sensitive data will be securely self-destructed after a data owner-specified expiration time. Secondly, user can access the data only one time from the cloud. At last, if the user enter the Incorrect key three times, the data will be self-destructed. Comprehensive comparisons of the security properties indicate that this scheme proposed by us satisfies the security requirements and is superior to other existing schemes.

Outsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. Sensitive data stored in the cloud must be protected from being read in the clear by a cloud provider that is honest-but-curious. Additionally, cloud-based data are increasingly being accessed by resource-constrained mobile devices for which the processing and communication cost must be minimized. Novel modifications to attribute-based encryption are proposed to allow authorized users access to cloud data based on the satisfaction of required attributes such that the higher computational load from cryptographic operations is assigned to the cloud provider and the total communication cost is lowered for the mobile user. Furthermore, data re-encryption may be optionally performed by the cloud provider to user environment while preserving the privacy of user data stored in the cloud. The proposed protocol has been realized on commercially popular mobile and cloud platforms to demonstrate real-world benchmarks that show the efficacy of the scheme. A simulation calibrated with the benchmark results shows the scalability potential of the scheme in the context of a realistic workload in a mobile cloud computing system. Secure deletion is the task of deleting data irrecoverably from a physical medium. In this work, we present a general approach to the design and analysis of secure deletion for persistent storage that relies on encryption and key wrapping.We introduce a generic update function and prove that it achieves secure deletion of data against a coercive attacker; instances of the update function implement the update behaviour of all arborescent data structures including B-Trees, extendible hash tables, linked lists, and others. We implement a B-Tree instance of our solution. Our implementation is at the block-device layer, allowing any block-based file system to be used on top of it. Using different workloads, we find that the storage and communication overhead required for storing and retrieving B-Tree nodes is small and that this therefore constitutes a viable solution for many applications requiring secure deletion from persistent media.

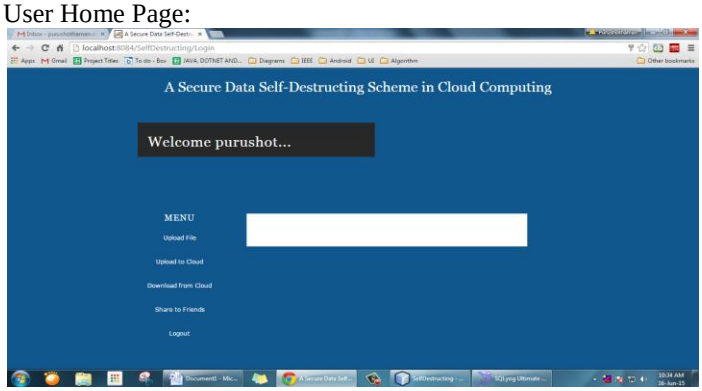
IV. RESULTS AND DISCUSSIONS



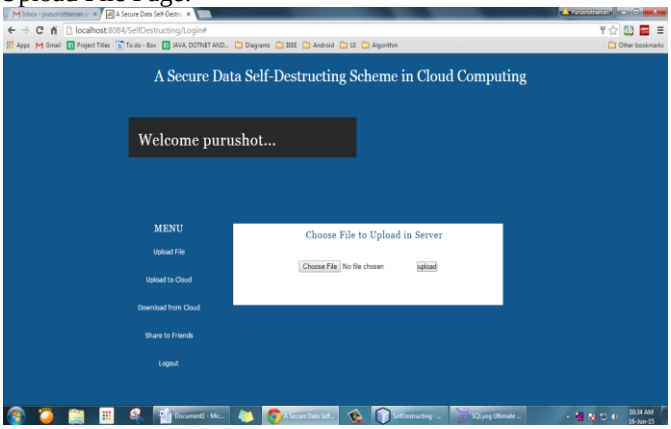
Registration Page:



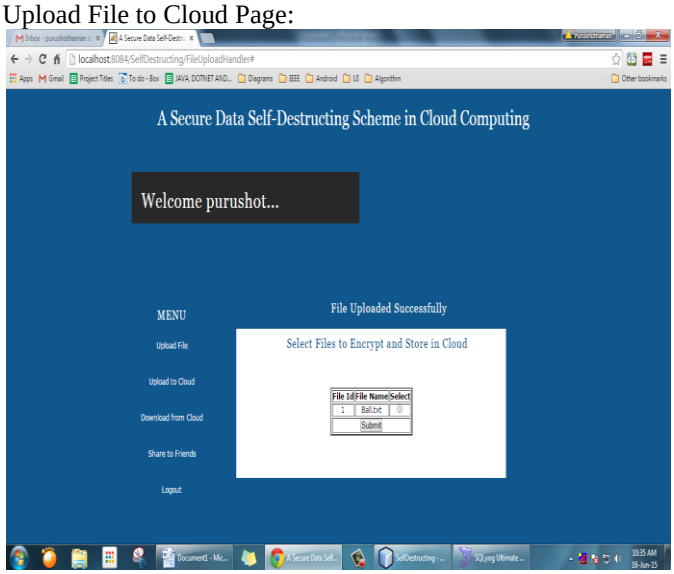
User Home Page:



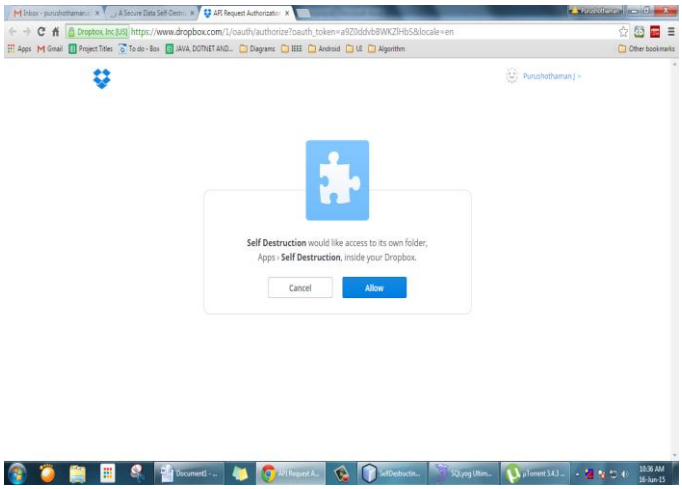
Upload File Page:



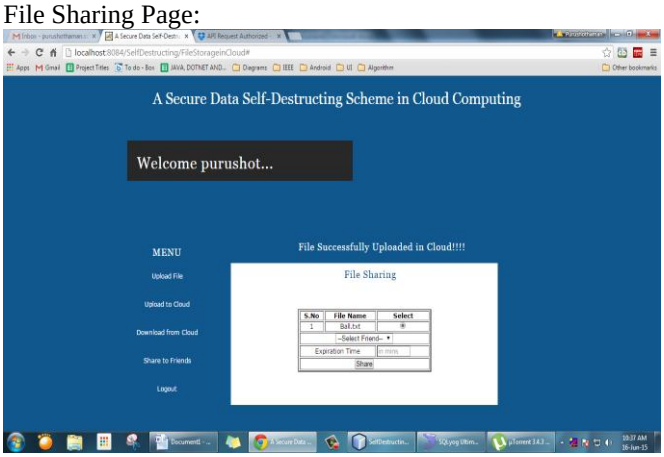
Upload File to Cloud Page:



Cloud Authentication:



File Sharing Page:



V. CONCLUSION

Since this project is all about Sharing files to friends perform computer actions the project has been designed keeping in mind the future scopes. What we have aimed and achieved creating is not a product but a tool to a better automotive environment, a tool can be used to shape many things in the future, thus this project will give rise to many future modifications forking in all directions. Some of the near future scopes of this project are as follows. There are few interesting problems we will continue to study for our future work. One of them is we can share a file to multi users at a time. We use AES (Advanced Encryption Scheme) to Encrypt the Data. In future we may develop this application using different types of Advanced algorithm for Encryption. We use Dropbox as a Cloud Server. In Future, we may developed that the user can select the Cloud Server such as Google Drive, Hostinger, Dropbox, AppBoxHe/She want.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditingfor shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.

[2] J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.

[3] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 142–157, 2013.

[4] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," Network, IEEE, vol. 28, no. 4, pp. 46–50, 2014.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and Communications Security. ACM, 2006, pp. 89–98.

[6] A. F. Chan and I. F. Blake, "Scalable, server-passive, user anonymous timed release cryptography," in Proceedings of the International Conference on Distributed Computing Systems. IEEE, 2005, pp. 504–513.

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

[8] L. Cheung and C. C. Newport, "Provably secure ciphertext policy abe," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 456– 465.

