ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (284-286), Month: January - March 2015, Available at: www.researchpublish.com

Fuzzy Security in Cloud Storage

[1]Gladwin A, [2]Amarnath S, [3]Arun Mozhi S.

[1,2,3] Department of Information Technology, Jeppiaar Engineering College, Chennai, India

Abstract: **On modifying Cipher text-Policy Attribute Based Encryption (CP-ABE) and OAuth, we propose a new security scheme, called fuzzy security, to facilitate an application registered with one cloud storage to access data available in cloud storage. The new proposed scheme enables the fuzziness of security to enhance the scalability and flexibility. Also, by conducting attribute distance checking and distance adjustment, operations like sending attribute sets and satisfying an access tree are eliminated. In addition, the automatic revocation is realized with update of Timeslot attribute when data owner modifies the data. In order to make an estimate of the performance of our scheme, we have implemented the protocol flow of fuzzy security with realized cryptographic part with Pairing-Based Cryptography (PBC) library.**

Keywords: **Fuzzy Security, Cipher Text-Policy, Security Scheme, Scalability and Flexibility.**

I. INTRODUCTION

The main use of cloud storage such as ease of accessibility and less physical space consumption, etc., have encouraged many people to use cloud services. Nowadays cloud services are gaining more importance in various fields. Due to this, the authorization between various cloud storages becomes a serious issue. For example, a data owner stores several Files inside cloud. Then, data owner wants to merge some of the files into one with the help of file Merger. The application File merger needs to be more secured to access the Files available in cloud storage. Another issue is that more than one secret key is needed if owner wants to authorize access right to

Several files. So that, a scheme which can address the security among different clouds and reduce the number of secret keys is required. By introducing a trusted authority to maintain the integrity of cloud applications, we propose fuzzy security for cloud storage which is an secure file-sharing scheme with high scalability and flexibility by modifying Ciphertext-Policy Attribute Based Encryption (CP-ABE). We propose a new secure security scheme for cloud storage providing file sharing tolerance, called fuzzy security. We have done the cryptographic part and simulated the protocol based on PBC library. The simulation gives the Fuzzy security to reduce the storage consumption compared to other similar possible security schemes.

II. RELATED WORKS

A chain of incipient access control schemes and solutions have been investigated and devised for cloud environment predicated on the general access control solutions. Due to its scalability and authenticity, Attribute-Predicated Encryption (ABE) gains the most popularity in the schemes for access control.

A distinguished work Fuzzy Identity-Predicated Encryption (IBE) was introduced by Sahai and Waters in 2005. In a Fuzzy IBE scheme, a private key for an identity set can be habituated to decrypt a cipher-text encrypted with a remotely different identity set. Fuzzy IBE realizes error tolerance by setting the threshold value of root node more minuscule than the size of identity set. Predicated on Fuzzy IBE, Goyal et al. present Key policy-Attribute Predicated Encryption (KP-ABE) and Bethencourt et al. introduce a complementary scheme to KP-ABE, called CP-ABE. There are more concrete and general CP-ABE constructions in a later paper.

On the other hand, Boneh constructed BB1 and BB2 approaches to build Identity-Predicated Encryption. Both CP-ABE and KP-ABE can be facilely acclimated to cloud environment, which has gained extensive researches along this line, verbally express [4, 20, 21], just to list a few. Tassanaviboon et al. propose an OAuth and ABE predicated sanction in semi-trusted cloud computing called AAuth. Their sanction method enables an owner-to-consumer encryption and fortifies encrypted file sharing without revealing owner's secret key to consumers by introducing a third party ascendancy. we propose FA in this paper which not only maintains the confidentiality and integrity of the data, but withal provides a scalable, efficient and flexible access control by modifying the general CP-ABE to habituate to the cloud storage environment. Through the integration of fuzzy functionality into the system, we enhance the scalability and flexibility of the secure sanction.

III. PROPOSED SYSTEM

By utilizing Fuzzy Sanction, we surmount the antecedent used OAuth protocol, which requires both resource data and accessing application to be in the same domain.

Another issue is that more than one access token or secret key is needed if owner wants to sanction access right of several files. Therefore, a scheme which can address the sanction among heterogeneous clouds and reduce the number of access tokens and secret keys is required. It is believed that OAuth is the most widely-adopted sanction scheme.

In Earlier, we used to download the files, which we update to utilize in other cloud storages. Now we surmount this by directly utilizing the files in the cloud between different cloud storages.

IV. SYSTEM MODEL

There are four main entities in the system.

Data owner: an entity who stores his/her data inside cloud storage and wishes to utilize cloud application accommodations to process the data. A data owner must register with cloud storage provider and must be logged-in in order to upload, access data or sanction.

Application accommodation provider (ASP): an entity to be sanctioned to access cloud storage data. It is an application software resides in vendor's system or cloud and can be accessed by users through a web browser or a special purport client software. For example, PDFMerge is an online implement which can be acclimated to merge several pdf files into one pdf file. With opportune sanction, PDFMerge fetches the source pdf files from cloud storage. As a result, uploading files from data owner's local contrivances eschewed.

Cloud storage provider (CSP): An entity which supplies storage as an accommodation to its clients and additionally provides access application programming interfaces (APIs) to ASP when ASP holds a valid access token. Dropbox and JustCloud mentioned antecedent are examples of such entity.

Application store (AS): an entity with which ASP must be registered to ascertain itself integrity and authenticity. Google Chrome Web Store is a typical application store.

Data owner encrypts his data with a desultory symmetric key KE and encrypts KE with our modified CP-ABE scheme. Since we accentuate the flexibility of multiple-file sharing, fuzziness is realized predicated on the file attributes. Once ASP gets all the indirect secret shares, it sends a request to CSP for formatted archive and then performs decryption of the archive header for KE. The main objective of this paper is to propose a secure and feasible way to address file-sharing issue with high scalability and flexibility in cloud storage.

V. SYSTEM TESTING

System testing is the stage of implementation which is aimed at ascertaining that system works accurately afore the live operation commences. During the development of a software project, errors of sundry types can occur at any stage. At each phase, different techniques are acclimated to detect the errors. The first major handle in the process of implementation procedure is the testing procedure.

To make the system development here to be reliable and accepted, sundry testing methods were utilized, the most fundamental of them being the three mentioned below.

Running the program to identify any errors (whether syntactic or semantic) that might have occurred while victualing the program into the system.

Applying the screen formats to regulate users to gauge the extent to which the screen was comprehensible to the utilizer.

Presenting the format to the administration for the purport of obtaining approbation and checking if any modifications have done or whether the proposed system accommodates their purport accurately.

VI. IMPLEMENTATION

Implementation literally betokens to put into effect or to carry out. The system implementation phase of the software deals with the translation of the design designation in to the source code and the internal documentation so that it can be verified facilely. The code and Documentation should be indited in a manner that cases debugging, test in and modifications. System flowcharts, sample run on packages, sample output etc, is a component of the implementation. Implementation is utilized here to mean the process of converting an incipient revised system design into an operational one. Conversion is one aspect of implementation.

VII. CONCLUSION

In this paper, we propose FA which carries out a flexible file-sharing scheme between an owner who stores his/her data in one cloud party and applications which are registered within another cloud party. The simulation of FA protocol proves that our scheme can prosperously adjust the attribute distance, expeditiously rectify the nonpareil indirect secret shares, resoundingly instaurate the top secret and then efficiently perform the decryption for KE. FA's self-distance-checking ability eliminates sending file attributes to ASP and distance-rectifying ability omits indispensability of performing gratifying the access tree procedure. The average time consumption of protocol amassed in our simulation implicatively insinuates that FA is at the same efficiency level as AAuth. The work was fortified by NSERC SPG and ORF RE.

VIII. REFERENCES

[1] http://www.thetop10bestonlinebackup.com/cloud-storage,2013.

[2] http://www.pdfmerge.com/, 2013.

[3] D. Balfanz, B. de Medeiros, D. Recordon, J. Smarr, and A. Tom, "The oauth 2.0 authorization protocol," Internet Draft, 2011.

[4] A. Tassanaviboon and G. Gong, "Oauth and abe based authorization in semi-trusted cloud computing," in Proceedings of the second international workshop on Data intensive computing in the clouds. ACM, 2011, pp. 41–50.

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

[6] R. McEliece and D. Sarwate, "On sharing secrets and reed-solomon codes," Communications of the ACM, vol. 24, no. 9, pp. 583–584, 1981.