International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34935-34938

Design and Development of Multilevel Authentication of Cloud Services Through De-duplication Mechanism

K. Saritha
PG Scholar,
Department of Computer Science and Engineering,
Nehru College of Engineering and research centre ,Pambadi,
Thrissur District,Kerala
Saru.rose123@gmail.com

Dr. S.Subasree
Professor and Head
Department of Computer Science and Engineering
Nehru College Of Engineering And Research Centre,Pambadi
Thrissur District,Kerala
drssubasree@gmail.com

Abstract- Data de-duplication is an important method for removing copied of similar data. It has been used in cloud to reduce the space of storage. To protect the data security differential authorized duplicate check is proposed.to improve the security of private cloud multilevel authentication is implemented, where security is based on providing password from the organization to the user of the data, with this the user is able to upload the data into the cloud. The proposed system provides more security than any other mechanism.

Keywords: Differential Authorized Check Scheme, Multilevel Authentication.

Introduction

Cloud service provides variety of services. As large data is uploaded into the cloud, the storage space utilization is more. In order to reduce number of data and to increase the storage space, de-duplication mechanism is proposed. De-duplication refers to repeated copies of similar data. In the De-duplication mechanism proposed earlier hybrid cloud architecture where private cloud and public cloud are included.in this mechanism differential authorized duplicate check is proposed, where the data uploaded into the cloud is checked for multiple copies, performing the duplicate check. The uploading of the file is based on set of privileges. The present de-duplication mechanism does not say anything about security. In the proposed work, multilevel authentication is implemented to enhance the security feature of the differential authorized de-duplication. In this more than three level of authentication is implemented. The first authentication is for the user. The second authentication is by the organization. The third is the team. Authentication is based on the creating new password .Our proposed work provides more security and support less overhead, the delay can be more as many level of verification are provided, but the security increases in this de-duplication mechanism.

Related Work

Whole file de-duplication in private cloud storage

The private cloud plays an important role in determining the duplication. The storage space has to be utilized to hold more amounts of data. It increases the storage space by providing space optimization and also increases the overall through put of the de-duplication mechanism. As a result large amount of data can be stored but security in that system is not that much concern [2].

Block level de duplication with encrypted data

The simple method of duplication is that data uploaded by various users will be stored only once if the content of the data is similar. The cloud de-dup mechanism which is proposed provides secure and efficient services to the de-duplication in the block level. Here it uses convergent encryption and an additional encryption operation along with access control mechanism. The convergent encryption technique meets the requirement of both the encryption and de-duplication. In the key is derived and encrypted based on the data provided. The key is result of the hash of the data segment. The CE results in the dictionary attack, which an attacker managed to, generate a key. By comparing the two cipher text it manages to get the file details. This technique produces a mechanism which gave protection against dictionary attack, but still result in loss of data due to lack in security. So security is not given to the data and results in attacks by the intruders, and the data is lost [3].

Trust model for file exchange in private cloud

In this it proposes the development of a high level trust worthy model for the file exchange among users in the private cloud. It is defined as an important factor for decision making in distributed and organized applications. Many trust models had been proposed by various scientist. Here the study of trust relationship between the trust security mechanisms to provide safe operation is a fundamental topic. It does not say anything about the authentication of users to make it secure. Computational trust can be used as it provide more advantages to the architecture and system monitoring still supporting scalability and security but the confidentiality of the data and the trust worthiness is not yet concerned [4].

Secure public cloud storage examining with de-duplication

Data reliability and useful storage are two major necessities for cloud storage. Here it tells to solve a problem based on the authentication tags .The proposed scheme is based on the communication and the cost .Here it allows duplication of both files and authentication tags. The scheme does not say anything about the security of the data [5]]

Identified Problem

In the existing de-duplication mechanism, we deliberate a hybrid cloud design comprising of public cloud and private cloud. The file is uploaded into the cloud based on the differential privileges of the user. The private cloud acts an

intermediate between the user and the public cloud. The file chosen by the user is based on their privileges.

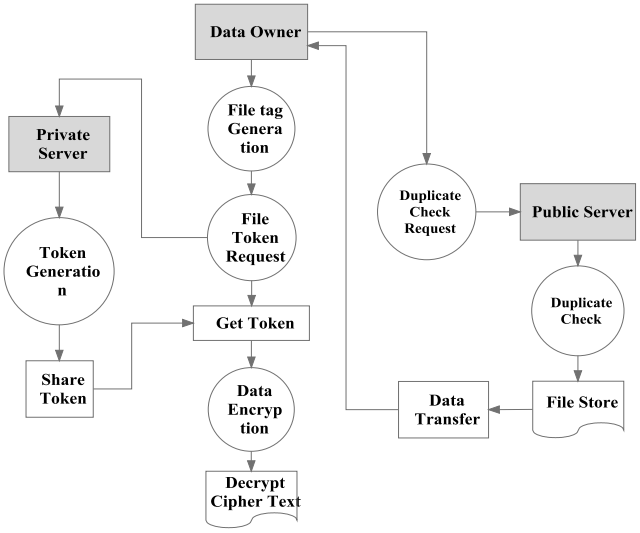

Figure 1.1: System Architecture

Security

The system provides less security. The private cloud which plays an important role in the de-duplication mechanism. The file that is selected by the user has to be uploaded to the public cloud. The tag and the token for each file is generated by the private cloud. The file is provided with less security.as a result an external intruder can get the file very easily. The existing system does not say anything about the authentication of each file.

Unexpected privilege escalation

The file is uploaded based on the certain set of privileges. The privileges are based on the two sets. They are the time based privileges and role based privileges. If the privileges are not correct, the file cannot be uploaded into the cloud.

Proposed Work

The proposed system uses the multilevel authentication .the authentication is separated into three basic levels. The first level authentication, the second level authentication and so on. The security of the private cloud is enhanced by providing this authentication mechanism. Finally, contrivance an archetype of the suggested technique in the variance endorsement duplicate check mechanism and conduct test bed experiments appraise the overhead of the archetype. We show that overhead is marginal associated to other security mechanism performed on the de-duplication mechanism.

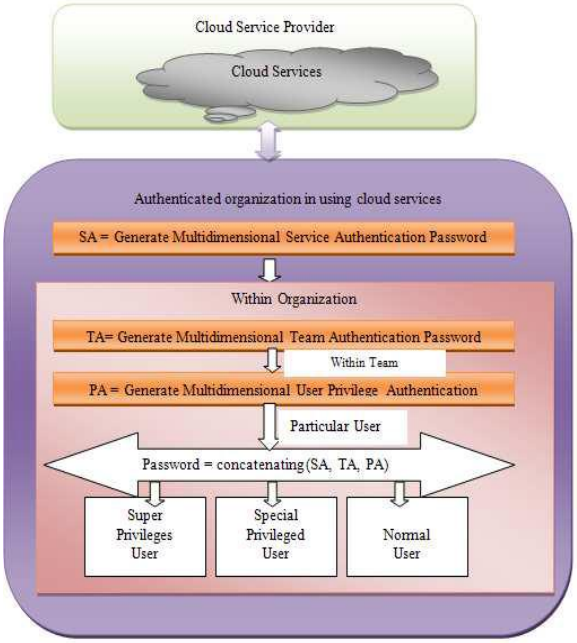

Figure 2: Architecture of multilevel authentication

Data owner description

The data owner is the person who registers in the data base. The user has to provide the credentials before they are selecting the files to upload.

Fig 2.1 Form of data owner

Organization description

In order to provide more security to the data, there are various sets of authentication level. The first level is the user level, the second level is the organization level and it goes on.

Fig 2.2 Form for the Organisation

Private and public cloud description

The private cloud plays an important role.The file selected by the user is send to the private cloud,where the token is generated and then uploaded into the public cloud .The duplicate check is performed in the public cloud.

Fig 2.3 Form for the Public Cloud

Result and Discussion

.Analysis of private cloud

In the case of private cloud, the file is selected based on the user, the data is saved. The rights of the file can be resolute which tells about its attributes, the name, time and the directory where the file is taken. It checks the database for the saved file. The rights are based on the time based and role based depend upon the attributes .The encryption algorithm is used to create the key with which the file is encrypted and it is being send. A tag formed for the file to detect the duplicate and the file is loaded to the public cloud.

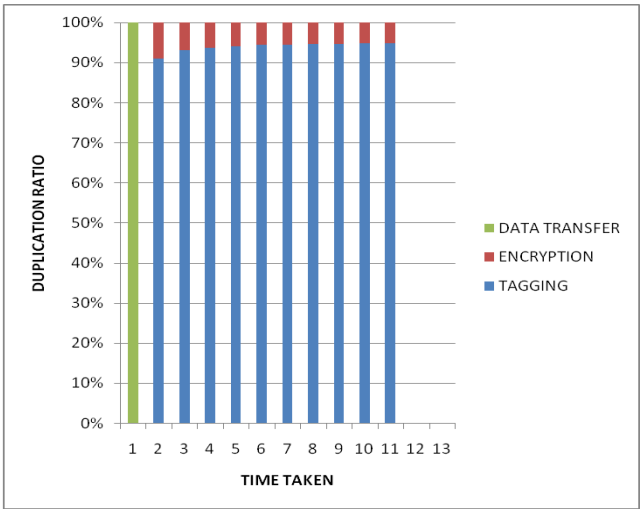

Fig 3 Time taken for the duplication ratio

The token for the file is generated and it will be shared to the data owner who is the user of the file. The information will be stored in the database and the files can be viewed. The properties of the file are shown and the path of the file is being chosen where it is being sent to the public cloud. To generate the token the path of the file is given along with the tag of the users file. The major drawback of this system is that less security is provided in the private cloud. Where it results in easy data loss and authentication of the user is not concern. To enhance the security we use the multilevel authentication technique.

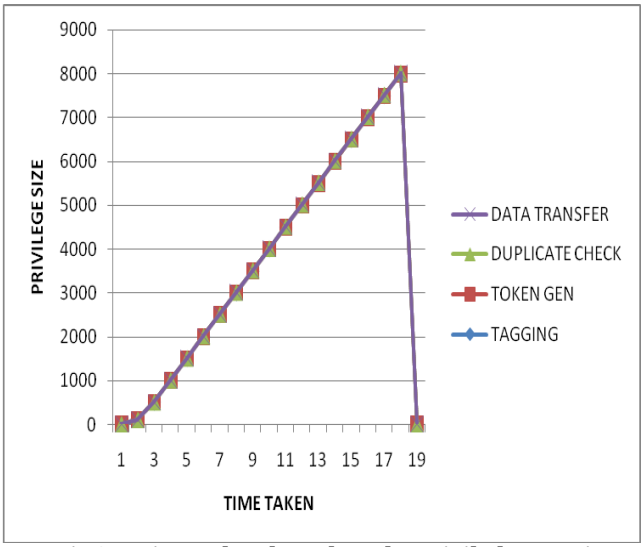

Fig 3.1 Time taken based on the priviledge set size

Analysis of public cloud

In the case of public cloud the duplication is being checked based on the tag of the file uploaded to the cloud. The file is kept in the cloud. The path is selected for the file and the file is being received. The content of the file is then verified to check the duplicates. The proof of owner ship determines the owner who is allowed to access the file. It duplicate is not there the file is stored in the cloud for further access, if the duplicate is there it has been allowed to inform the user who is uploading the file. The public cloud is used where the data has to uploaded.It checks the duplicates if similar data are present.

The graph represents the break down time taken for the file which is being uploaded by the public cloud based on the key generated by the private cloud.An identification protocol is used based on the proof and verfiy.A user determines his individuality to a verifier by performing the proof correlated to the identity.The input is the private key that he is used to share with the user.The verifer performs the confirmation with input of unrestricted evidence.At the end of the protocol the verifer.

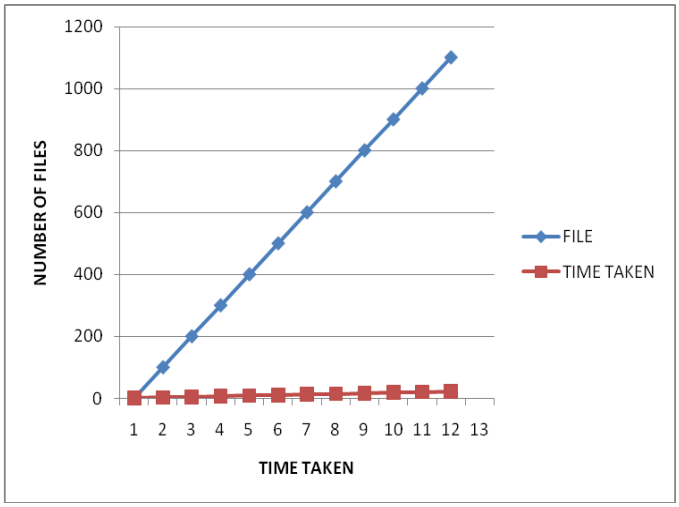

Fig 3.2 Break down time taken for each file

.Analysis of public and private cloud

The private cloud and the public cloud is analyzed where the performance of the private cloud is analyzed as security is less in the case of private cloud. To enhance the performance and to increase the security multilevel authentication is proposed someplace the certification is built on the three stages that is the organization level, team level and the user level. The delay in such case is less and security is more compared to other existing authentication techniques like graphical password and biometric authentication .The client side of the system support the token generation and duplication along with the file upload. The file tag is used to determine the tag with the file. The Tokenreq is used to request the private server for the generation of token with the file tag and id of the user. The dupcheckreq is used to request the storage server for identical check. The sharetokenreq is used to generate the share file token. Both public cloud and private cloud of the hybrid system is being analyzed and found out that less security is provided in this approach. As a result multilevel authentication is provided to improve the security of the private cloud in the hybrid approach.

Conclusion

In this paper, multilevel authentication anticipated to safeguard the data safekeeping in the private cloud which checks the files and saves the file based on the particular privilege provided by the user, security analysis shows that our outline are secure in terms of various attacks by the outsiders. As a result we implement an archetype of our projected multilevel authentication mechanism and conduct experiments. .As a result to provide more security to the private cloud we use the multilevel authentication technique. The files before uploading into the public cloud is checked for duplication based on the data operation performed by the private cloud. The nominal which is produced by the remote cloud before uploading will be authentication by the organization and then the team for further providing the security. The organization level authentication is based on the privileges provided by the organization for the user. This mechanism is highly secure against brute force attack and other passive attacks. We showed that our mechanism increases the security, though delay is there, but it increases security and reduces the minimal overhead of the de-duplication mechanism.

References

[1] K.Saritha, Dr.S. Subasree " Analysis of Hybrid Cloud Approach for private cloud in the De-duplication Mechanism".

[2] M.Shyamala Devi, V.Vimal Khanna and A.Naveen Bhalaji "Enhanced Dynamic Whole File De Duplication for space optimization in private cloud, Vol 4, August 2014.

[3] A.Pasquale Puzi, B.Refik Molva "Bloak level De-Duplication with Encrypted Data "OGCC Vol 1, 2014.

[4] Edna Dias Canedo,Rafael Timoteo de sousa, "Trust Model For Reliable File Exchange in Cloud Computing" Vol. 4, Feb 2012

[5] Jiawei Yuan, Shucheng Yu " Secure and constant cost public cloud storage Auditing with De-Duplication ".

[6] Jin ji , yan ki li,Patrick P.C " A Hybrid Cloud Approach for Secure Authorized De-Duplication " IEEE Vol PP No : 99 2014.

[7] Dinesh H.A, Agrawal V.K "Multilevel Accessing Technique For Cloud Service "Vol 2, 2012.

[8] OpenSSL Project. http://www.openssl.org/.

[9] P.Anderson and L.lang "Fast and Secure Laptop Backups With Encrypted De-Duplication. In Proc of USENIX LISA 2010.

[10] M. Bellare, S. Keelveedhi, and T. Ristenpart. Dupless: Server Aided Encryption for De-Duplicated Storage. In *USENIX Security Sym*, 2013.