International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 10th Febraury 2018. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-7&issue=ISSUE-02

Title: A Hybrid Cloud Approach For Secure Authorized Deduplication

Volume 07, Issue 02, Page No: 156 – 160.

Paper Authors

***YADLAPALLI NAGA KALYANI, V. NAGA GOPI RAJU.**

* Dept of CSE, Chalapathi Institute of Technology.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A HYBRID CLOUD APPROACH FOR SECURE AUTHORIZED DEDUPLICATION

[1]YADLAPALLI NAGA KALYANI, [2]V. NAGA GOPI RAJU
*PG Scholar, Dept of CSE, Chalapathi Institute of Technology, Guntur
**Assistant Professor, Dept of CSE, Chalapathi Institute of Technology, Guntur

ABSTRACT: In this paper we are going to discuss about the hybrid cloud approach process to reduce the bandwidth and storage space. To eliminate the duplicate copies which is occurred due to reapeated data we use an data compression techniques that is data deduplication technique. Basically, to protect the data while dedulpication we use an encryption technique that is convergent encryption technique. The main purpose of this technique is to encrypt the data before utilising. So in this paper we are going to discuss about how to protect the data in more efficient way by authoirising the problem of deduplication.Here differential previleges of users are consisdersd in the duplicate check beside the data. Now in hybrid cloud architecture we are constructing new deduplications that supports the authoroised duplicate check scheme. By using the prototype it implements our proposed authorised duplicate check scheme.

I.INTRODUCTION

To hide the platform and implement the details of users, cloud computing is one of the main technique. The cloud services provides higly available stotage and parallel computing resources at low cost. As cloud comuting is increasing in todays world, in the same way the large amount of data also begins to store in the cloud and shared by the users with some previliges. One of main problem of cloud computing is to manage the data. Basically, to manage the data in cloud computing we uses an efficiuent technique that is deduplication. Data duplication is an data compression technique which is used to elininate the duplicate copies in the storage. The main purpose of the technique is to improve the the storage utilization and applied to the network data transforms which reduces the number of bytes. Here the deduplication technique will eliminates the redundant data. The deduplication process is at the file level opr at the block level.coming to the file level deduplication, the duplicate copies will be eliminated of same file and in the same way at the block level of deduplication, the duplicate blocks will be eliminated from non identicxal files.

Deduplication process not only eliminates the duplicate copies but also provides the secuirty and privacy. Data deduplication secures the users data from both insider and outsider attacks. This proposed technique provides the data confidentaility and in the same wayit encrypts the data with their own keys. This deduplication process become impossible when the identical copies of different users leads different cipher text. So to overcome this problem a convergent encryption technique is proposed.

The main intent is to enforce the data confidentiality. By using a convergent key the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

data will encrypts or decrypts. Now this is computed by a hash value with some content of data copy. After this data encryption and key generation process, the user will retain the key and sends to the cipher text to cloud. So in this paper we are going to solve the problem of deduplication with different privileges in cloud computing. By using the hybrid cloud architecture this process is obtained. In this hybrid cloud architecture they are both public and private clouds. Here the private cloud allows the data owner to perform duplicate check securely with different privileges. Here the data owners will outsource the data storage by using public cloud. Now a new deduplication system with differential duplicate check is proposed in hybrid cloud approach. In this this hybrid cloud approach the user is only allowed to perform the duplicate check for files. For better security purpose we enhance an advanced encryption system with different privileges . Now the authorised users cannot decrypts the cipher text with S-CSP. Here the proof of ownership is important so in this it enables the user to prove their ownership of data copies to the storage server. Next step is to identify the protocol. It is done in two phases one is proof and another one is to verify. From this all processes we can say that the proposed hybrid approach secures the data in an efficient way.

II. EXISTED SYSTEM

As we know that the one of the important technique to eliminate the duplicate copies is data deduplication technique. This data deduplication technique is also known as data compression technique. This technique is most widely used in the cloud storage to reduce the amount of storage space and as well as to save the bandwidth. In this technique the cloud computing provides the virtualized resources to the user to protect the data confidentiality. So the existed system provides the data with low cost and reduce the storage space. But it is not efficient and thee data is not managed properly. For that purpose an system is proposed which is given below.

III. PROPOSED SYSTEM

Basically, deduplication is the well known technique to manage the data in cloud computing and data deduplication is the data compression technique which is used to eiminate the data which is occurred due to repeated data. But in existed system the main disadvantage is deduplication is impossible and in the same way the data is susceptible to both insider and outsider attacks. To overcome this a system is proposed that is convergent encryption technique. This technique enforces the data confidentiality.The entire process of proposed system involves three steps mainly system set up, file uploading and file retrieving which are discussed below in a particular format.

By using a convergent key it encrypts and decrypts the data. This key is obtained from the hash value with some content of data copy. After the key is generated and encrypted user will retain keys and send the cipher text to the cloud. This can be generated from the data encryption opeartion which is deterministic. To overcome the unauthorised access a secured ownership protocal isneeded. Now the user

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

should need a proof that he uses the same file when the duplicate one is used.

After the process of proof, the user with same file will provide a pointer from the server without the need to upload the same file. Now the user can download the encrypted file with pointer from the server. But this can be decrypted by the corresponding data owners with some convergent keys. Now this convergent encryption will allow the cloud to perform the dulpication on ciphertext. Compared to past, the previous deduplication systems cannot support the differntial authorization duplicate check. So at last we can say that in the authorised deduplication system, a set of previliges are issued to the user during system initialization. The each file is uploaded to the cloud by set of previliges. So the main advantage of this proposed system is that data confidentaility is maintained and compared to existed system this proposed system secures the data in very efficient way. The syttem architecture is shown in below figure (1).

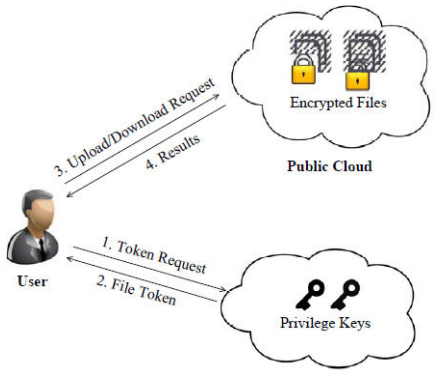

FIG. 1. ARCHITECTURE FOR AUTHORISED DUPLICATION

Up to nowwe have discussed about the system thee proposed system operation but now let us discuss about the evaluation of proposed system. Generally the evaluation of prototype from file token generation and share token generation is done by using different factors which are given as 1. File size, 2. Number of stored files, 3. Deduplication ratio and 4. Privilege set size. Now all these experiments ate conducted with three machines they are intel core 2-Quad 2.66 GHz, core Quad cpu, 4 GB RAM and installed with ubuntu 12.04 32 bit operation system. All these machines in the system are connected with 1Gbps ethernet neetwork. After this upload process is done in six steps which are given as 1. Tagging 2. Token generation. 3.duplicate check 4. Share token generation 5. Encryption 6. Transfer. For every step there will be start and end time notification. Let us discuss about the different factors which are evaluated

1. File size

By uploading 100 unique files with particular file size we can evaluate the file size and record the time breakdown. But here the time which is spent on tagging, encryption, upload will increase the file size linearly.

2. Number of stored files

In the same way as earlier we need 100 10MB unique files to upload the files and it records the breakdown of every upload then we can evaluate the effect of number of files.

3. Deduplication Ratio

Here two unique data sets are prepared in the system which consists of 50 100MB

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

files. By this way we can evaluate the effect of deduplication ratio.

4. Privilege set up

By uploading 100 10 MB unique files with different size of data owner and previlige set size, then wee can evaluate the effect of previlige set size.

Atlast we can conclude that the data security is processed and evaluated in an efficient way in proposed hybrid approach system. This system occupies low storage space and the cost is also very low compared to the existed one.

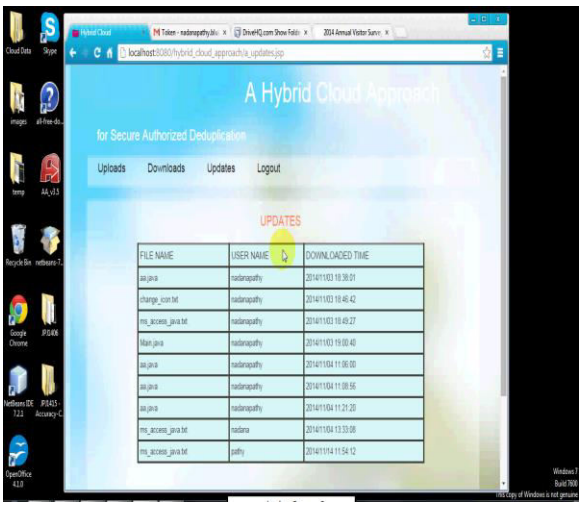

FIG. 2. RESULT

IV. CONCLUSION

Here first an data deduplication process is proposed to protect the data security with different privileges. But this process doesn't secures the data in an efficient way. So a new deduplication process is proposed that is hybrid cloud approach. This hybrid cloud architecture consists of duplicate check token files which are generated by private cloud with private keys. From the analysis of security we can say that the data is protected from the insider and outsider attacks. Coming to the proof of ownership, it is implemented by a prototype which consists of authorised duplicate check scheme. Compared to the existed system the proposed system occupies low storage space and consists of low cost.

V. REFERENCES

[1] Charles. Roth Jr., "Digital Systems Design using VHDL", Thomson Brooks/Cole, 7th reprint, 2005.

[2] S. S. Kerur, Prakash Narchi, Jayashree C N, Harish M Kittur and Girish V A, "Implementation of Vedic multiplier for Digital Signal Processing", International Conference on VLSI, Communication & Instrumentation (ICVCI) 2011, Proceedingspublished by International Joural of Computer Applications® (IJCA), pp.1-6.

[3] Himanshu Thapaliyal and M.B Srinivas, "VLSI Implementation of RSA Encryption System Using Ancient Indian Vedic Mathematics", Center for VLSI and Embedded System Technologies, International Institute of Information Technology Hyderabad, India.

[4] Jagadguru Swami Sri Bharati Krishna Tirthaji Maharaja, "Vedic Mathematics: Sixteen simple Mathematical Formulae from the Veda", Delhi (2011).

[5] Harpreet Singh Dhillon and Abhijit Mitra, "A Reduced-bit Multiplication Algorithm for Digital Arithmetic", International Journal of Computational and Mathematical Sciences, Febrauary 2008, pp.64-69.