International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Multilevel Cryptosystem for Authorized Deduplication in Hybrid Cloud

P. Narasimhulu[1], Jayavarthini .C[2]

[1]Department of Computer Science Engineering, SRM University, Chennai, India

[2]Assistant Professor in Department of Computer Science, SRM University, Chennai, India

Abstract: ***Data deduplication is the one of necessary data compression technique, for eliminating redundant copies of data in the cloud. It has been widely used in cloud storage; eliminating redundant data can significantly shrink storage requirements and improve bandwidth efficiency. To support data confidentiality for the sensitive data. Attribute based encryption has been implemented along with multilevel crypto system, encrypt the data before outsourcing and protect better security for the data in the cloud, In this paper makes the first attempt to formally addressing the problem of authorization of data deduplication. Different users consider duplicate check in the data itself. We also implement several new duplications systems supporting authorized duplicate check in hybrid cloud architecture. Security analysis explains about the secured terms in the proposed security model. We show that our proposed duplicate check scheme incurs minimum overhead compare to normal operations***

Keywords: Data deduplication, multilevel cryptosystem

1. Introduction

Cloud computing that mainly works on sharing computing resources rather than having local servers or personal devices to handle applications. Perhaps, the most significant cloud computing benefit is in terms of IT cost savings exist and while keeping capital and working cost to a nominal. With cloud computing, you can save substantial capital costs with zero in-house server storage and application storage requirements. Outsourcing the data in cloud for storage has become an attractive trend due to the increase in cloud computing technology. Due to this cloud has main critical objection of cloud storage services is the management of the ever-increasing volume of data.

To maintain data in cloud computing is archival through data depulication. This technique often called as "intelligent compression" or single-instance storage is a method of decreasing storage needs by eliminating redundant data. Only one unique instance of the data is actually retained on storage media. Related and somewhat synonymous terms are intelligent compression and single-instance storage. Many organizations use duplications in backup and disaster recovery applications, but it can be used to free up space in primary storage as well. Deduplication can also decrease the amount of network bandwidth required for backup processes, and in some cases, by using deduplication we can boost the backup and recovery process.

Even if data deduplication brings lot of advantages, it mainly concrete on privacy and security concerns. Sensitive data are protectable to both outside and insider attacks. Convergent encryption provides privacy and security with data confidentiality is incompatibility with deduplication. But implementing convergent encryption data users produce with single convergent key along with cipher text. Thus unauthorized will access the key, it may lead chance to mislead the data into the cloud. Key sharing also main disadvantage to the convergent encryption. Users may confuse with this deduplication. Multilevel cryptosystem has been introduced for data confidentiality and key sharing. Multi Key will generated thorough attribute based encryption with that encryption technique user will access the key. That key may be generated through user registration process.

If the users want to access the key, he/she will get it through the mail id, and from that the he/she can access the data. However, previous deduplication systems cannot support different authorization check, each users are issued with set of privileges during the process of deduplication. Before user uploading a file into the cloud is also bounded with bunch of privileges to specifies which kind of user accessing the files and checking the files in the cloud, Although multi cryptosystem provides confidentiality to some extent, it will not support do not encourage duplicate check with different privileges, It seems to be contradiction if we want to access both deduplication and different authorized check at same time

2. Contributions

In this paper, aiming at effectively solving problems on deduplication with different privileges in cloud computing, and we considering hybrid architecture with public and private cloud. Finally, we implement a key that proposed before outsourcing the data into the cloud with attribute based encryption and file upload operations. And proposed a practical deduplication system.

3. Preliminaries

3.1 Convergent Encryption:

With the convergent encryption, we get data confidentiality of deduplication. Data owner receives a data copy of convergent key along with the tag. Tag is used to detect the duplicate copy. Here tag can't reduce the convergent key and compromise data confidentiality, below functions can define convergent encryption scheme

- KeyGenCE (m): Data copy m to convergent key k.

- EnCE (K, M): Input as M and output with cipher text c;
- DeCE (K, C): K as input and output will be original data M;

3.2 Multilevel cryptosystem and attribute based encryption:

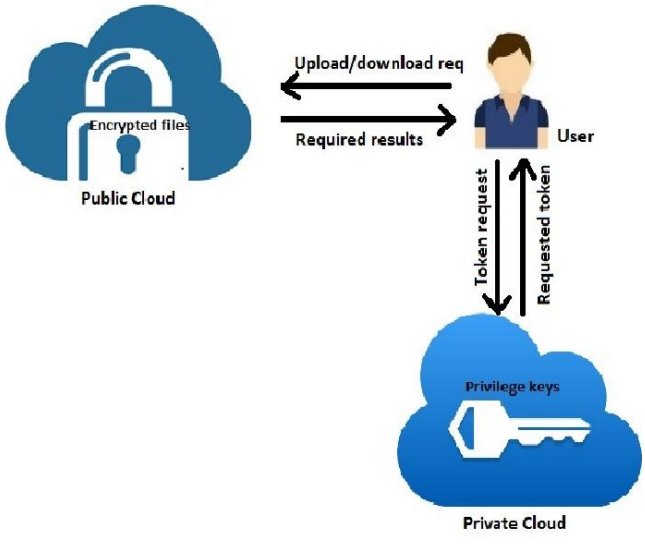
In the concept of multilevel cryptosystem we provide multilevel security for the data with perfect keys before data will be outsourcing in the cloud, Basically we providing multilevel keys(K) and that keys will be made from attribute based encryption. It mainly produce the keys from user details, after entering the keys only user will performs action in the cloud with help of data depulication

4. System Model

4.1 Hybrid Architecture for Secure Deduplication

In this particular setting, deduplication can be widely implemented in this architecture. Backup and disaster recovery applications made great impact on reducing storage space. Such systems are greatly often suitable to user file backup and synchronizations applications than richer storage abstractions.

Private cloud will produce the keys and data will outsourcing in the public cloud, the access right to a file is defined as the set of privileges, Users will access the private cloud sever and mainly user token request also send to the private cloud only. Now we will explain the process of architecture, User will send a token request to the private cloud sever for outsourcing the user data in to the cloud. From that scenario privilege keys are generated and that will be transformed to the user, the major portion has been starts after producing keys only. Specifically to upload/download request has been executing by the public cloud , After verifying the privilege keys user will access the cloud and he encrypts/decrypts or update action will be performed. In the encryption process data deduplication will be performed, it can easily reduce redundant copies of data in the cloud .Here duplication performs two type of actions file-level duplication and block-level duplication and each data is associated with a token for duplicate check.



4.2 Adversary Model

Typically, both public cloud and private cloud are honest. All files are sensitive based on the data and their possessions, Files are protected by both public and private cloud for that we have consider two kinds of adversaries they are:

(1) External adversaries: It mainly aims the extract the secret information as much as possible from public and private cloud.

(2) Internal adversaries: Aim to obtain more information on the file from public cloud and duplicate check information from the private cloud.

5. Proposed System

5.1 Problem

- When unauthorized user gets to know the key, he can decrypt everything with that key.s
- Key sharing.
- In the existing system they proposed only single key has generated and that key is using before outsourcing the data into the cloud.
- Reduce the storage size of the tags for integrity check. To enhance the security of deduplication and protect the data confidentiality.

5.2 Objective

An advance system has been proposed, which will make effective on cloud storage. Multi crypto system has been implemented along with attribute based encryption with that technique no key sharing and we will make control on the UN authorized users. User want to encrypt/decrypt the data is very easy manner that's compare with the previous techniques.

5.3 Solution

Deduplication is the only process that eliminates redundant copies of data in the cloud, and we propose an advance deduplication system supports unauthorized duplicate check. In this deduplication system we introduced hybrid cloud architecture is used to solve the problem. The private keys are not generated directly and not issued to the user, which will be managed by the private cloud server.

In this process the users cannot share the set of private keys. It plays impact on the set of key sharing privileges. To get file token, the user send a request to the private cloud server, Construction of key/token generation as follows. The private cloud server will check the user identity before issue the corresponding token to the user. The authorized duplicate check for file can be perform by the user with help private cloud server.Before construction of key/token after verifying user's identity key will be generated according user details with help of attribute based encryption technique. Upload the data before outsourcing data into the cloud user need to enter the key, multi keys are generated and that keys are user's mail after seeing the key user's need enter the key in public cloud after verifying the key the cloud will check on the

deduplication after completion of deduplication process the data will upload in the cloud. Encrypt/decrypt process can be done through AES algorithm from that scenario user's will not going for key sharing and we will prevent the un authorized visit into the cloud .The private cloud will maintain the keys with corresponding privileges ,the file storage system will present in the public cloud.

6. Design Description

Detailed information about the architecture has been showed in the figure; five different modules are present in the proposed system. The detail of the module has given in the below:

(1) Setting private cloud.
(2) Token generation.
(3) Validating the token.
(4) To achieve deduplication by encrypting file before encrypting.
(5) Validating the token before decrypting.

7. Multi Level Cryptosystem

Mostly commonly for achieving for confidentiality, and reducing the key sharing. Cryptosystem mainly consist of three systems

1. Key generation.
2. Encryption.
3. Decryption.

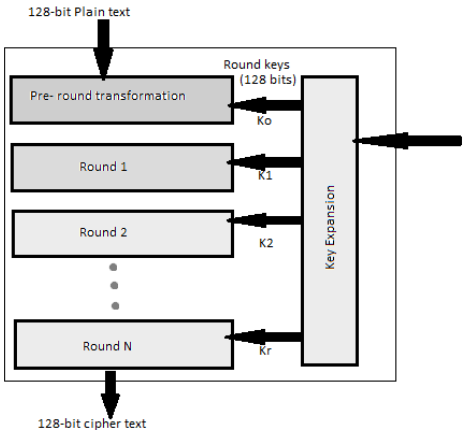
7.1 Attribute based encryption

It is most powerful encryption technique, Attribute based encryption is a kind of process public key generation along with the secret key. The key will generated from user attributes. . In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

7.2 AES Algorithm

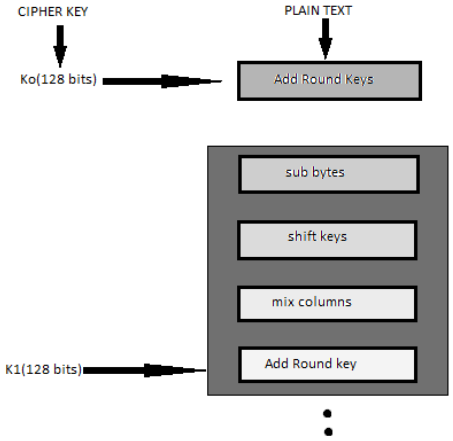
AES performs all its computations on bytes rather than bits. Hence, AES takes a 128 bit secret key and it combines it with plaintext blocks which are arranged in four columns and four rows for processing as a matrix. This is called cipher text.

But in DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, and it takes 9 loops for 10 rounds. Likewise 12 rounds for 192-bit keys with 11 loops for 12 rounds.And finally 14 rounds for 256-bit keys, with 13 loops for 14 rounds. Each of these rounds uses a different 128-bit, 192-bit and 256-bit round key respectively, which is calculated from the original AES key.



Encryption Process

The description of a typical round of AES encryption is given below.Each roundcomprise of four sub-processes. The first round process is depicted below:



Situated from a fixed table given in design. The result will be in a matrix, which consists of four rows and four columns.

2) Shift rows: Each four rows of the matrix are shifted to the left. Shift is carried out as below-

- First row is not shifted.
- Second row is shifted to one (byte) position to the left.
- And third row is shifted two positions to the left from right.
- Fourth row is shifted three positions to the left.
- The resulting is a new matrix consisting of the 16 bytes, but shifted with respect to each other.

3) Mix Columns

Each column of four bytes is converted by using a special mathematical function. This function takes an input of four bytes of one column and produces an output, which is four completely new bytes, which replaces the original column. And the result will be another new matrix, which consists of 16 new bytes. It should be noted that this step is not performed in the last round.

4) Add round key

The 16 bytes of the matrix are now considered as 128 bits and are XOR'ed to the 128 bits of the round key. If this is the last round then the output is the cipher text. Otherwise, the resulting 128 bits are interpreted as 16 bytes and another similar round.

Decryption Process

The decryption process for an AES cipher text is exactly the reverse order of the encryption process. Each round consists of the four processes taken place in the reverse order −

•Add round key
•Mix columns
•Shift rows
•Byte substitution

Since the decryption process is in reverse manner, the encryption and decryption algorithms should be separately implemented, although they are related very closely.

8. Security Analysis

Our system have been designed to solve the different privileges problem in deduplication, the security check will be maintain through in term of two aspects ,the authorization of duplicate check and confidentially of data .Based up on two terms we show that system are secure with the follow security analysis

1) Security of duplication check
2) Confidentially of data

9. Conclusion and Future work

In this paper introduces the Transpose-Minify Framework Which is important programming model for next-generation distributed systems, namely cloud computing.In this paper presented the different impacts of the Transpose-Minify model in the computer science discipline, along with different efforts around the world. It can be observed that while there has been a lot of effort in the development of different implementations of Transpose-Minify, there is still more to be achieved in terms of Transpose-Minify optimizations and implementing this simple model indifferent areas. The future work of this paper is performing the optimizations using the Transpose-Minify Frame work.

References

[1] OpenSSL Project, (1998). [Online]. Available: http://www. openssl.org/
[2] P. Anderson and L. Zhang, “Fast and secure laptop backups with encrypted de-duplication,” in Proc. 24th Int. Conf. Large Installation Syst. Admin., 2010, pp. 29–40.
[3] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Dupless: Serveraided encryption for deduplicated storage,” in Proc. 22nd USENIX Conf. Sec. Symp., 2013, pp. 179–194.
[4] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in Proc. 32nd Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2013, pp. 296–312.
[5] M. Bellare, C. Namprempre, and G. Neven, “Security proofs for identity-based identification and signature schemes,” J. Cryptol., vol. 22, no. 1, pp. 1–61, 2009.
[6] M. Bellare and A. Palacio, “Gq and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks,” in Proc. 22nd Annu. Int. Cryptol. Conf. Adv. Cryptol., 2002, pp. 162–177.
[7] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, “Twin clouds: An architecture for secure cloud computing,” in Proc. Workshop Cryptography Security Clouds, 2011, pp. 32–44.
[8] J. R. Douceur, A. Adya, W. J. Bolosky, D. Simon, and M. Theimer, “Reclaiming space from duplicate files in a serverless distributed file system,” in Proc. Int. Conf. Distrib. Comput. Syst., 2002, pp. 617–624.
[9] D. Ferraiolo and R. Kuhn, “Role-based access controls, ” in Proc. 15th NIST-NCSC Nat. Comput. Security Conf., 1992, pp. 554–563.

Author Profile

P.Narasimhulu currently pursuing M.Tech degree in SRM University (Computer Science department). Heattended a National level conference on “An Estimated distance based routing protocol for mobile ad-hoc networks” advance computing and published a journal.

C. Jayavarthinireceived ME degree from Francis Xavier Engineering College, Tirunelveli in 2011.Currently, she works in SRM University as an Assistant Professor. Her research interests include Data mining, DBMS, Web Mining. She attended various international conferences on DBMS.