

Design and Implementation of a Hybrid Cloud Approach for Secure Authorized Deduplication

Satish Khadke
Department of Computer
Engineering
Aditya Engineering College,
Beed

Sayyed Mustafa
Department of Computer
Engineering
Aditya Engineering College,
Beed

Syed Akhtar
Department of Computer
Engineering
Aditya Engineering College,
Beed

ABSTRACT

Data deduplication began to emerge approximately ten years ago, but has only recently become an important technology and also it is one of the important data compression techniques to eliminate duplicate copies of data. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. Here new deduplication constructions supporting authorized duplicate check in this hybrid cloud architecture are presented. Security analysis demonstrates that our scheme is secure in terms of the definitions specified in the proposed security model. We show that our proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

Keywords

Authorized duplicate check, deduplication, hybrid cloud, private cloud, public cloud, security algorithms

1. INTRODUCTION

Cloud computing is the recent technology which is widely used to implement business applications as well as scientific applications. It is an efficient method to manage lots of servers, databases, and networking of large organizations. More than a decade ago, engineers find out the ways in which data and software could be distributed effectively over several systems and their power pooled for collective use.

Cloud computing provides on-demand delivery of resources and everything is through internet with pay-for-use basis. Failure to ensure appropriate security protection when using cloud services could directly result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing. Customer must have clear understanding about security using cloud computing. There are different types of services namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each model provides different security requirements and responsibilities. There are many security risks like compliance and legal risk, authentication and authorization, ambiguity, and many more. To tackle these some techniques need to be composed in basis systems.

1.1 Public Cloud

A public cloud based on the standard cloud computing model and it is accessed by any subscriber with an internet connection and access to the cloud space. In public cloud, a service provider makes resources, such as storage and applications and it is available to public over internet. Public model may be free for all or may be pay-for-use.

1.2 Private Cloud

A private cloud which is established for a specific group or organization and it limits access to just that group. Its implementation aims to avoid many of the conflicts about cloud computing security. Because setup of private cloud is implemented safely within the corporate firewall, it also provides more control over the company's data, and it ensures security.

2. RELATED WORK

Security becomes a big concern when we store important information on a platform and which is not directly controlled by the user and which is far away [8]. When data is sent and while storage data is under threat because any unauthorized user can access it and may modify it, so there is a need to secure data. If following three conditions are satisfied, then we can say data is secured: (i) Confidentiality (ii) Integrity (iii) Availability. Confidentiality means the data is understandable to the receiver only for all others it would be waste; it helps in preventing the unauthorized disclosure of sensitive information. Integrity means data received by receiver should be in the same form, the sender sends it; integrity helps in preventing modification from unauthorized user. Availability means give assurance that user can access information anytime and to any network. In the cloud confidentiality is obtained by cryptography.

2.1 Data Encryption Standard (DES)

DES algorithm is very commonly used as symmetric key algorithm. It was developed by IBM in 1974, but now a days many methods are found that had proven this algorithm unsecured [1].

In DES algorithm, block cipher is of 64 bits [2] and out of 64 bits of keys, 56 bits key is used and rest of 8 bits are padded.

In block cipher, we first encrypt the data which encrypted block of data consists of plain text by combination of confusion and diffusion which makes cipher block. After this cipher block has to pass 16 rounds, before passing through these 16 rounds the 64 bits of data is divided into 32 bits. After dividing the data into 32 bits, F-function (Feistel function) is applied. F-function consists of substitution, permutation, key mixing. The output of function is combined with other half of the data using XOR gate alternate crossing of data is done; then crossing of data is done.

2.2 Advance Encryption Algorithm (AES)

Advance Encryption algorithm (AES) is also known as Rijndael. In AES algorithm, various size of key is used i.e. 128, 192 or 256 bits, depending on how many cycles it uses [3]. For 10 cycles, 128-bit key, 12 cycles, 192 bit key and for 14 cycles, 256 bit key is used. Except last one, all the cycles

of AES are similar. It works on 4x4 matrixes. AES consists of following three stages as- key expansion, initial and final round. Initial round consist of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key and final round also consists of similar function as initial round except mix columns. AES works fast on both software and hardware.

2.3 RSA

RSA was invented by Ranold Fivest, Adi Shamir and Leonard Adleman in 1977[6]. RSA is an asymmetric algorithm. Functioning of RSA is based on multiplication of two large numbers. In RSA, two large prime numbers are generated and multiplied. After multiplying these two numbers, modulus is calculated and the number that is generated is used as the public and private key [9]. The two numbers that are used for

multiplication-one of them is public other is private. Steps for RSA algorithm are as follows:

- Divide the large message into small number of blocks where each block represents the same range.
- By raising the eth power to module n encrypt the message.
- For the decryption of message increase another power d module n.

3. SYSTEM ARCHITECTURE

Following diagram shows the basic system model working. Here, if the user operates public cloud the data/files are encrypted and in case of private cloud data/files are operated using privileged key and then user get the results after these respective processing.

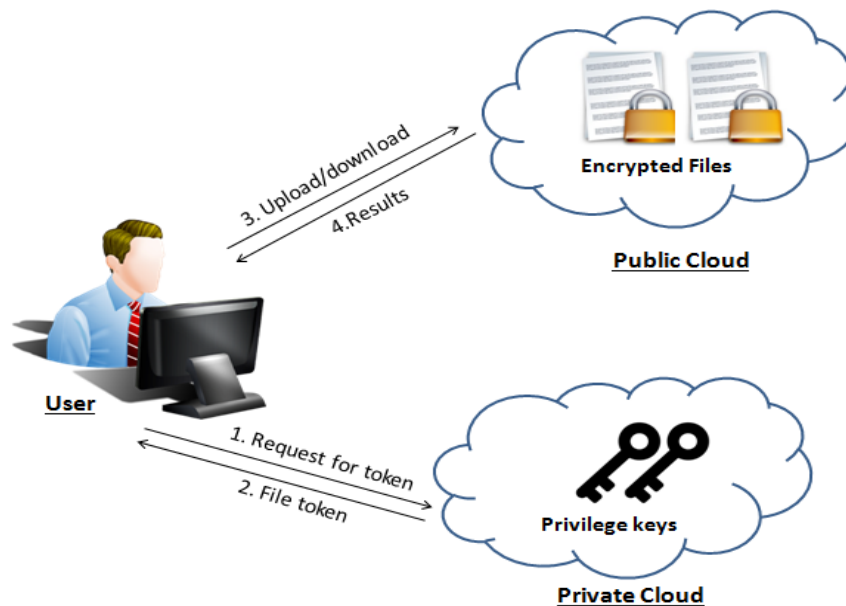


Fig 1: Authorized Deduplication

3.1 Working

- User can apply login credentials.
- Admin
 - Admin will approve disapprove the User request for login credentials.
 - If admin approves the request then following details will send to the user.
 - Username
 - Password
 - Secret pin to download and delete file.
 - If admin disapproves the request then user record will be deleted and disapprove mail will send to the user.
- User can upload the file.
- User can delete his own file by using secret pin.
- On Upload following operation will happen to achieve **Deduplication**.
 - Hash Code generation on the basis of content of the file.
 - If same hashcode exists in database table then pointer will set to the existing file.
 - If hashcode is unique then file will be uploaded as a new entry.
- On Delete following operation will happen-
 - User provides secret pin on rise of delete request.
 - If file has any pointer then only database entry will be deleted.
 - If there is no pointer to the file then its a unique file and database entry and file both will be deleted.
- On Download following operation will happen-
 - User provides secret pin on rise of download request.
 - If secret pin matched then only file will be downloading.

4. ALGORITHMS

4.1 Advanced Encryption Standard (AES)

AES algorithm is used to encrypt the data. It is consists of three block ciphers, AES-128, AES-192 and AES-256. Here

each cipher block encrypts and decrypts the data in the block size 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. AES consists of following three stages as- key expansion, initial and final round. Initial round consist of Add Round Key, Sub Bytes, Shift Rows, Mix Columns, Add Round Key and final round also consists of similar function as initial round except mix columns. AES works fast on both software and hardware.

4.2 Secure Hash Algorithm (SHA)

On the basis of file content, SHA generates hash code. Cryptographic hash functions are mathematical operations run on digital data by comparing the computed "hash" to a known and expected hash value, a person can determine the data's integrity. For example, compute hash of downloaded file first then compare the hash of previous published hash result and check whether downloaded file is modified or not.

4.3 Input/output

4.3.1 Input

- Login credentials.
- File that is to be uploaded.
- Secret pin on download and delete request.

4.3.2 Output

- Upload encrypted file
- Hashcode of the file.
- Download decrypted file.

Hybrid Cloud Approach

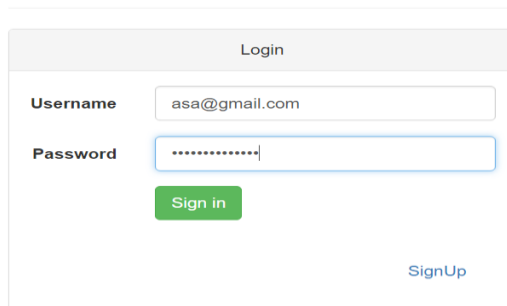


Fig 2: User Login Page

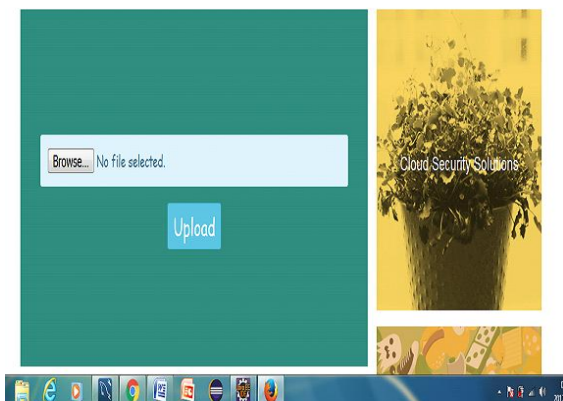


Fig 3: Upload File Page

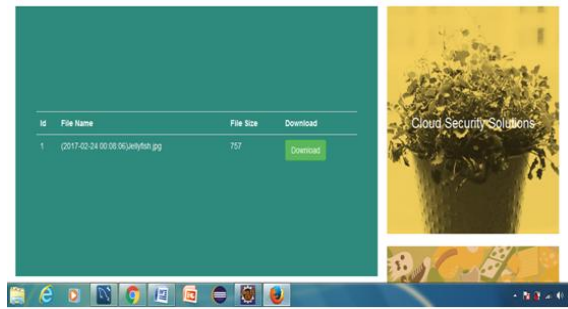


Fig 4: Download File Page

5. CONCLUSIONS

In this paper we implement the hybrid cloud approach and proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

6. REFERENCES

- [1] Jawahar Thakur and Nagesh Kumar, 'DES, AES Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis', International Journal of Emerging Technologies and Advanced Engineering(IJETAE), December(2011), ISSN: 2250-2459 Vol. 1, Issue 2.
- [2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Neha Jain and Gurpreet Kaur, 'Implementing DES Algorithm in Cloud for Data Security', VSRD International Journal of CS & IT. (2012), Vol.2 Issue 4, pp. 316-321.
- [3] Rachna Jain and Ankur Aggarwal 'Cloud Computing Security Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. January (2014) Vol. 4, Issue 1.
- [4] Pratap Chandra Mandal, 'Superiority of Blowfish Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering. September (2012) ISSN: 2277-128X Vol. 2, Issue 7.
- [5] Sandipan Basu, 'International Data Encryption Algorithm (IDEA) - A Typical Illustration', Journal of Global Research in Computer Science. July (2011) ISSN: 2229-371X Vol. 2, Issue 7.
- [6] B.Persis Urbana Ivy, Purshotam Mandiwa and Mukesh Kumar, 'A Modified RSA Cryptosystem Based on 'n' Prime Number', International Journal of Engineering and Computer Science. Nov (2012) ISSN: 2319-7242 Volume 1 Issue 2.
- [7] Ayan Mahalanobis, 'Diffie-Hellman Key Exchange Protocol', Its Gernalization and Nilpotent Groups. August (2005).
- [8] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. (2011).
- [9] Shakeeba S. Khan and Prof. R.R. Tuteja, 'Security in Cloud Computing Using Cryptographic Algorithms', International Journal of Innovative Research in Computer and Communication Engineering. January 1, (2015) ISSN (online): 2320-9801, (Print): 2320-9798 Vol. 3.

- [10] Maha TEBA, Said EL HAJJI and Abdellatif EL GHAJI, 'Homomorphic Encryption Applied to the Cloud Computing Security', World Congress on Engineering, July 4 (2012) Vol. 1, London U.K. ISBN: 978-988-19251-3-8, ISSN: 2078-0958 (Print); ISSN: 2078-0966 (online).
- [11] G. Devi and M. Pramod Kumar, 'Cloud Computing: A CRM Service Based on a Separate Encryption and Decryption using Blowfish Algorithm', International Journal of Computer Trends and Technology. (2012) Vol. 3 Issue 4, ISSN: 2231-2803, pp.592-596.
- [12] Manzoor Hussain Dar, Pardeep Mittal and Vinod Kumar, 'A Comparative Study of Cryptographic Algorithms', International Journal of Computer Science and Network. June (2014) ISSN(Online): 2277-5420, Volume 3, Issue 3.