International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Possession of Provable Multi-Copy Dynamic Data in Cloud Computing Systems

Y. Sunil[1], C. Hasya[2]
MCA Student[1], Assistant. Professor[2]
Mother Theresa Institute of Computer Applications, Palamaner, S. V. University, Andhra Pradesh, India

Article Info
Publication Issue :
Volume 8, Issue 6
November-December-2022
Page Number : 90-94
Article History
Accepted: 01 Nov 2022
Published: 05 Nov 2022

ABSTRACT

A key strategy for the cloud service provider to ensure data availability is replication. Numerous multi-copy integrity auditing systems were introduced to give consumers persuasive proof that the copies they need are all kept appropriately. However, with this scheme, we demonstrate that the scheme is easily vulnerable to copy-summation attacks and single-copy attacks, wherein a dishonest CSP just has to invest a single copy's worth of storage costs in order to always pass the verifier's challenge. As a result, in this instance, the scheme is no longer secure.

Keyword: MR-PDP, DES, AES

I. INTRODUCTION

The global cloud computing market is anticipated to rise from $272billion in 2018 to $624billion by 2023 at a compound annual growth rate of 18%, a report from research and markets showed. Cloud computing is an advanced technology every person is used inner or outer in today's world. The advance and rapidly expanding technology of cloud computing are used computation and storage. The very minimum cost is used storage and computation as a service in it. Service model provided three essential services in it: infrastructure as a The suggested method uses a dynamic PDP strategy in a storage system that uses replication and hides the CSP's architecture from users. Liu et al. introduced a dynamic multi-copy audit system that employs a novel tree structure to cut down on bandwidth and calculation expenses for each audit. We demonstrate that the modified version is vulnerable to a single-copy attack, whereas the two versions [5] are vulnerable to a copy- summation attack. A cheating CSP can always pass the verifier's challenge by using the copy-summation attack, which requires it to merely save the sum of all copies for each block. Since the original file cannot be reconstructed from the total of the copies, this violates the integrity of the data. By using the copy-summation attack, a cheating CSP just has to keep track of the total number of copies for each block in order to pass the verifier's test at any moment. Since the original file cannot be reconstructed from the total of the copies, this violates the integrity of the data. By using the single-copy attack, a dishonest CSP can maintain just one copy while tossing the others, but it can still utilise the copy that was kept and its verification tags to get a legitimate proof for a different copy. As a result, the degree of data availability that customers demand is significantly reduced. In essence, the two assaults mentioned above defeat the scheme's primary objective.

II. RELATED WORKS

Multiple-Replica Provable Data Possession (MR- PDP)

To enhance the availability and longevity of data on unreliable storage systems, many storage systems rely on replication. As of right now, these storage technologies offer no conclusive proof that numerous copies of the data are truly kept. Storage servers can work together to conceal the fact that they are only storing one copy of the data while giving the impression that they are keeping multiple copies. We fix this flaw in several ways. MR- PDP: replica proven data possession Using a challenge- response protocol, a client that saves t copies of a file in a storage system may confirm that (1) each unique copy can be made at the time of the challenge and (2) the storage system utilises t times the storage needed to store a file. For a single copy of a file in a client/server storage system, the MR-PDP builds on earlier work on data possession proofs. It is computationally considerably more effective to store t replicas using MR-PDP than it is to store t independent, unconnected files using a single- replica PDP approach (e.g., by encrypting each file separately prior to storing it). Another benefit of MR- PDP is that when some of the existing duplicates fail, it can produce additional replicas on demand and inexpensively.

Mirror: Providing evidence of data retrievability and replication in the cloud

A cloud provider can demonstrate that data is correctly saved in the cloud using cryptographic methods called Proofs of Retrievability (POR) and Data Possession

Top-down levelled multi-replica MuR-DPA Secure public auditing based on a Merkle hash tree for cloud-based dynamic large data storage

This restricts the business models that for replicas.

Possession of dynamic, dispersed, and transparent data

Summary:
I have discovered from this that, It enables actual situations where the cloud storage provider (CSP) may conceal its internal organisation from the customer and flexibly manage its resources while still offering the client a service that can be independently verified. The number and types of servers used to hold the data are determined by the CSP. We find one to two orders of magnitude improved performance in our testing due to the spread load.

Possession of proven multicopy dynamic data in cloud computing systems

Organizations are choosing to outsource data to distant cloud service providers in increasing numbers (CSPs). By paying costs metered in gigabytes/month, customers can rent the storage capacity of the CSP to store and retrieve almost infinite amounts of data. Some clients may like to have their data duplicated over numerous servers and data centres for a higher level of scalability, availability, and durability. Customers pay greater fees when the CSP is required to keep more copies. Customers must thus have a solid assurance that the CSP is storing all data copies specified in the service contract and that all such copies are accurate as of the most recent customer revisions. The map-based proven multicopy dynamic data possession (MB-PMDDP) approach that we provide in this study has the following characteristics: 1) It gives clients proof that the CSP is not deceiving them by maintaining fewer copies; 2) it supports outsourcing of dynamic data, i.e., it supports block-level operations, such as block modification, insertion, deletion, and append; and 3) it allows authorized users to seamlessly access the file copies stored by the CSP. We give a comparative analysis of the proposed MB- PMDDP scheme with a reference model obtained by extending existing provable possession of

dynamic single-copy schemes. The theoretical analysis is validated through experimental results on a commercial cloud platform. In addition, we show the security against colluding servers, and discuss how to identify corrupted copies by slightly modifying the proposed scheme. This article taught me that 1) it supports outsourcing of dynamic data, i.e., it supports block-level operations, such as block modification, insertion, deletion, and append; 2) it supports block-level operations, such as block modification, insertion, deletion, and append; and
3) it enables authorised users to easily access the file copies stored by the CSP. We compare many aspects of the MB-PMDDP system that has been presented.

III. Methodology

Proposed system:

In the replication-based storage system, where the CSP's architecture is concealed from users, we have presented a dynamic PDP approach. a dynamic multi-copy audit technique that supports dynamic data and makes use of a map-version table and a novel tree structure to cut down on bandwidth and computation expenses for each audit. The method can be significantly altered to determine which copy is faulty.

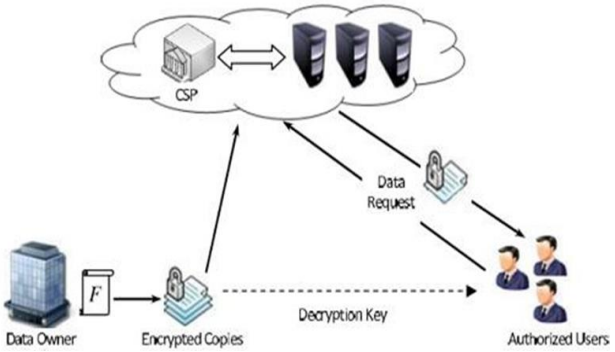

Figure 1: block diagram

IV. Implementation

This project is implemented by using below mentioned algorithm called Advanced Encryption Standard.

Advanced Encryption Standard

The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.

A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows –

• Symmetric key symmetric block cipher
• 128-bit data, 128/192/256-bit keys
• Stronger and faster than Triple-DES
• Provide full specification and design details
• Software implementable in C and Java
Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

Unlike 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, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –

Encryption Process

Here, we restrict to description of a typical round of AES encryption. Each round comprise of four sub-processes. The first round process is depicted below –

Byte Substitution (SubBytes)

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows

Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows –

• First row is not shifted.
• Second row is shifted one (byte) position to the left.
• Third row is shifted two positions to the left.
• Fourth row is shifted three positions to the left.
• The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns

Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

Decryption Process

The process of decryption of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order –

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

Since sub-processes in each round are in reverse manner, unlike for a Feistel Cipher, the encryption and decryption algorithms needs to be separately implemented, although they are very closely related.

AES Analysis

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of

key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

V. Conclusion

The dynamic multi-copy public auditing technique in [5] was examined in this letter, and it was demonstrated that the construction is weak to both the copy-summation attack and the single-copy assault. More specifically, a dishonest CSP just has to expend the storage effort required to save a single copy in order to succeed, yet the verifier cannot catch

them. To remedy this, we provided a corrected scheme that can thwart the two assaults as well as some straightforward but effective countermeasures.

VI. REFERENCES

[1]. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiplereplica provable data possession," in Proc. 28th Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411–420.

[2]. F. Armknecht, L. Barman, J. M. Bohli, and G. O. Karame, "Mirror: Enabling proofs of data replication and retrievability in the cloud," in Proc. 25th USENIX Secur. Symp., 2016, pp. 1051–1068.

[3]. M. Etemad and A. Küpçü, "Transparent, distributed, and replicated dynamic provable data possession," in Proc. 11st Int. Conf. Appl. Cryptogr.Netw.Secur. (ACNS), 2013, pp. 1–18.

[4]. C. Liu, R. Ranjan, C. Yang, X. Zhang, L. Wang, and J. Chen, "MuR-DPA: Top-down levelled multi-replica Merkle hash tree based secure public auditing for dynamic big data storage on cloud," IEEE Trans. Comput., vol. 64, no. 9, pp. 2609–2622, Sep. 2015.A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485–497, Mar. 2015.

[5]. G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[6]. K. Zeng, "Publicly verifiable remote data integrity," in Proc. 10th Int. Conf. Inf. Commun. Secur. (ICICS), 2008, pp. 419–434.

[7]. Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

Cite this article as :

Y. Sunil, C. Hasya, "Possession of Provable Multi-Copy Dynamic Data in Cloud Computing Systems", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 90-94, November-December 2022.
Journal URL : https://ijsrcseit.com/CSEIT22865