Acta Scientific COMPUTER SCIENCES

Volume 5 Issue 3 March 2023

Research Article

Possession of Identity-Based Distributed Verifiable Data in Several Cloud Storage

Dipali Prakash Patil*, Amruta Deshmukh, Chandrani Singh and Ankush Kudale

Department of Computer Sciences, India

***Corresponding Author:** Dipali Prakash Patil, Professor, Department of Computer Sciences, India.

Received: January 30, 2023

Published: February 14, 2023

Abstract

In cloud storage, remote data integrity testing is quite important. Without downloading the entire data set, it can force the clients to confirm that their outsourced data has been preserved. The clients may need to store their data on multi-cloud servers in certain application scenarios The integrity checking procedure must be effective to save the verifier money at the same time. Researcher formulate a unique remote data integrity checking paradigm based on these two points: Multi-cloud storage with ID-DPDP (identity-based distributed provable data possession). Given are the formal system model and security model. Using the bilinear pairings as a foundation, a specific ID-DPDP protocol is created. According to the conventional CDH (computational Diffie- Hellman) problem's hardness assumption, the proposed ID-DPDP protocol is demonstrably safe. Our ID-DPDP protocol is effective and adaptable in addition to the structural benefit of eliminating certificate administration. The proposed ID-DPDP protocol can implement private verification, delegated verification, and public verification depending on the client's authority. Event facts are accurate, disposition checking is to be copied, and ID-DPDP identity-based produced distribution obvious information for computers property) is being stored in several clouds. A solid, unique, ID-DPDP certified style is intended. The entire dress event system style to be traced and safety style to be traced are given by the linear pairings. The proposed ID-DPDP signed international agreement may be secure under the laboriousness constraint associated with the common CDH (computational Diffie- Hellman) hard question. A proposal ID-DPDP signed agreement between nations will note non-public verification, gave powers verification, and public verification. In addition to trying to structure better chances of elimination of statement of fact as authority business managers, our IDDPDP approved style is also wise at making an impression and versatile supported the customer's authority.

Keywords: Cloud Computing; Security; Computational Diffie-Hellman; Identity-based

Introduction

Information will be kept in the multi-cloud utilising the ID-DP-DP protocol (Identity-based distributed demonstrable information possession). The IDDPDP protocol eliminates certificate management. This approach spreads the client's data among a number of cloud servers that can manage its size and structure. The non-public key that the non-public key generator generates for the customer contains their unique ID. Information from the client is received by the combiner, which distributes it according to data volume and kind. The challenge is delivered via the voucher to the combiner, who then transfers it to the respected cloud. The outcome is then combined, and the combiner decides if it is valid or not. Permit customers to store the data in various clouds if it's valid.

Information will be stored in the multi-cloud using a protocol called ID-DPDP (Identity-based distributed demonstrable information possession). The IDDPDP protocol does away with certificate administration. In this method, the client's data is dispersed to multiple cloud servers that can handle its size and format. The consumer's unique ID is contained in the non-public key that the non-public key generator produces for them. The combiner re-

ceives the client's information and distributes it in accordance with the volume and kind of data. The challenge is transferred to the revered cloud by the combiner after being sent by the voucher to the combiner. The result is then combined, and the combiner determines whether or not it is valid. Allow buyers to store the data in many clouds if it's valid. Inside the section Extract, PKG creates the non-public key for the consumer. The block-tag attempt is created by the consumer and uploaded to the combiner. In accordance with the storage data, the combiner distributes the block-tag pairs among the various cloud servers. The challenge is sent by the voucher to the combiner, who then distributes it to the appropriate cloud servers in accordance with the storage data. The challenge is answered by the cloud servers, and the combiner then compiles these answers from the cloud servers. The aggregative response is sent to the voucher by the combiner. The voucher then verifies the validity of the aggregate response. The signature, possession of demonstrable knowledge, and distributed computing are the primary sources of the concrete ID-DPDP structure. The signature links the client's non-public key and identity. Computerized sharing is employed to store the client's information on multi-cloud servers. At the identical time, distributed computing is additionally accustomed mix the multi-cloud servers' responses to retort the verifier's challenge. supported the demonstrable information possession protocol, the ID-DPDP protocol is built by creating use of the signature and distributed computing.

Related work

Remote information integrity checking is a significant security flaw in cloud computing. Large amounts of client information are not under his control. The information of the client may be corrupted by the malicious cloud server in order to gain many benefits. The corresponding system model and security model were planned by numerous researchers. The PDP paradigm for demonstrable information possession was first presented in 2007 [3]. The voucher will almost certainly check the integrity of remote information under the PDP model. They created two indubitably secure PDP algorithms that supported the RSA. Next, a dynamic PDP model with a concrete theme was developed, albeit insert operations were not supported [2]. Erway intended a full-dynamic PDP theme that supported the attested flip table in 2009 to allow the insert operation [4]. F.Seb'e [5] has additionally completed work along these lines.

PDP allows a voucher to validate the accuracy of remote data without actually obtaining or downloading it. By selecting a random sample of server blocks, it provides a probabilistic proof of ownership that significantly lowers I/O costs. To carry out the integrity verification, the voucher only keeps a small amount of data. A motivating paradigm for distant information integrity verification is PDP. The protection mechanism and specific theme of proxy PDP publicly clouds were planned by Wang for 2012 [6]. The cooperative PDP within the multi-cloud storage was planned by Zhu at the same time [7]. The following models and protocols for remote information integrity checking are planned. Additionally, F.Seb'e [5] completed Shacham.work in 2008 [8-20].

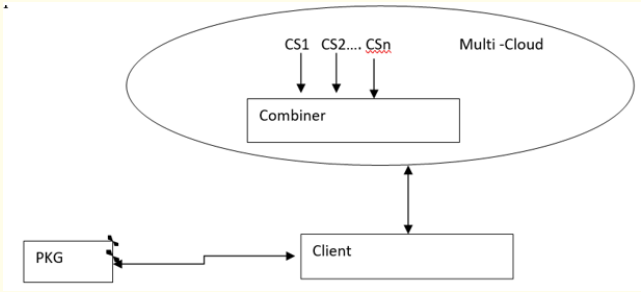

Figure 1

Methodology

The most popular project management methodologies in the field of project management are as follows:

- Secure Key process
- Verification Generator
- Server processing
- Information Assurance to User method
- Admin Auditing Model

Existing system

The location of the data on the cloud is mobile because it is stored in numerous places. The location of the user's data on the cloud may or may not be known to him. Because the cloud is multi-tenant, a user may need to sign in using separate user credentials for several providers. In the event that the login credentials are misplaced or leaked outside of the system, anyone could pretend to be the original owner, posing a threat to the data. To encourage greater transfers to the cloud, a cloud must have a reliable identity and access management system in place.

System requirement

- Cloud computing uses Identity-Based Encryption with Outsourced Revocation for security.
- In this project Encryption/Decryption is used to secure the data.

Problem statement

A significant portion of data breaches are brought on by the careless or unintentional release of sensitive data rather than a deliberate attack. Employees frequently share, allow access to, mishandle, lose, or share valuable data either accidentally or because they are unaware of security procedures.

Employee education as well as other methods like data loss prevention (DLP) technology and improved access controls can be used to solve this serious issue.

Social engineering attacks such as phishing and others.

Attackers frequently utilise social engineering techniques to get access to confidential information. They entail coercing or deceiving people into divulging personal information or granting access to restricted accounts.

One such method of social engineering is phishing. There are messages that appear to be from a trusted source, but in fact are sent by an attacker. When victims comply, for example by providing private information or clicking a malicious link, attackers can compromise their device or gain access to a corporate network.

The objective of system

In cloud storage, remote data integrity testing is quite important. Distributed verifiable data possession is a crucial component of distant data security in a multi-cloud scenario. In multi-cloud storage, we provide an unique remote data integrity checking methodology called ID-DPDP (identity-based distributed provable data possession). According to the computational Diffie Hellman problem's hardness assumption, the suggested ID-DPDP protocol is demonstrably safe. The ID-DPDP protocol under consideration enables private, delegated, and public verification. Improve security by providing. Achieved through designing user-friendly data entry panels that can manage enormous amounts of data. Better protect personal data, such as passwords, credit card and debit card information, etc.

Contributions

Module 1: Owner

Our first model is the owner, the owner can select a text file and upload it after uploading the file this file is split into three parts, and then these three-part will be encrypted separately by applying DES Algorithm with the key and he also send the key on the email of the verifier and also upload the encrypted file on the server.

Module 2: Verifier

The public verifier can correctly check the integrity of shared data. The public verifier can audit the integrity of shared data from multi-cloud with whole Data and accept the file. In this module public auditor check all file's integrity And accept the files to the cloud.

Module 3: Private key Generator

A person or thing outputs the appropriate private key when it receives the identity.

The signature, possession of verifiable data, and distributed computing form the core of the concrete ID-DPDP structure. The signature links the client's private key and identity. The client's data is stored on multiple cloud servers using distributed computing. Additionally, distributed computing is employed to integrate the responses from the several multi-cloud servers in order to reply to the challenge posed by the verifier. The ID-DPDP protocol is built using the signature and distributed computing and is based on the verifiable data possession protocol.

Symmetric key

Encryption is the conversion of data (plain text) into a secret code, and it uses a symmetric key (Cipher Text). It is the best method for achieving data security. The ability to read an encrypted file is required. The best method for achieving data security is through encryption. You need to have access to a secret key or password that can decrypt an encrypted file in order to read it. Text is referred to as data. Cipher text is the name for encrypted data.

Symmetric key encryption

Symmetric Key Encryption is a type of encryption where the same keys are used to both encrypt and decode data.

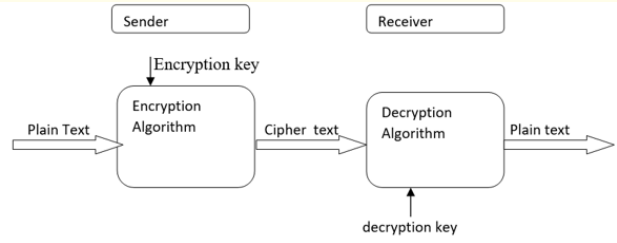

Figure 2: Symmetric key.

Asymmetric key encryption

Asymmetric Key Encryption is a type of encryption in which different keys are used to encrypt and decrypt data. It is possible to recover the plaintext by decrypting the cypher text despite the fact that the keys are distinct yet mathematically linked.

Module 4: User

Each user registers their user information for using files in this module. A cloud server's login page is only accessible to registered users. The user can examine a block of uploaded files that have been approved by cloud servers and verified by a verifier on the multi-cloud server in this module. This module enables the user to download an uploaded file that has been authenticated by a verifier using his identification key before being downloaded from a multi-cloud server.

Module 5: Cloud Server

To keep the data of the clients, a managed entity by the cloud service provider has a sizable amount of storage and computing capacity. Each server from the multi-cloud module verifies the file block in this module and accepts the block of files for the verifier to validate.

Background and related work

Data encryption standard (DES)

It is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though the key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). The General Structure of DES is depicted in the following illustration.

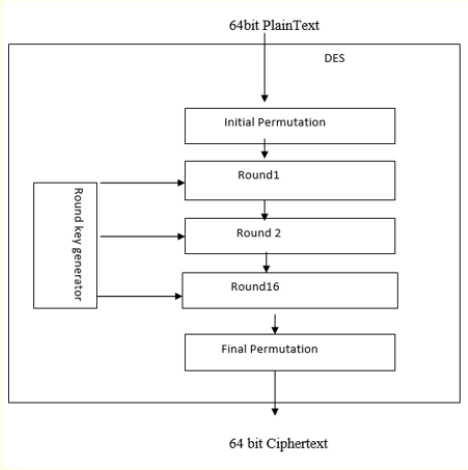

Figure 3: DES.

Since DES is based on the Feistel Cipher, all that is required to specify DES is:

- Round function
- Key schedule
- Any additional processing – Initial and final permutation

Review method

Initial and Final Permutation

The initial and final permutations are straight Permutation boxes (p-boxes) that are inverse of each other.

Round function

The heart of this cipher is the DES function, The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

Expansion permutation box

Since the right input is 32-bit and the round key is 48- bit, we first need to expand the right input to 48 bits.

Straight permutation

The 32-bit output of S-boxes is then subjected to the straight permutation with the rule.

Key generation

The round-key generator creates sixteen 48-bit keys out of a 56-bit cipher key.

Conclusion

It is obvious that even if the use of cloud computing has grown quickly, cloud computing security is still seen as the main problem in the ecosystem. Customers don't want malicious insiders in the cloud to steal their confidential data. Additionally, a significant number of consumers have recently experienced numerous issues as a result of the loss of service availability. Additionally, data intrusion causes a lot of issues for cloud computing customers. This research aims to review current security utilising multi-cloud research. We discovered that while cloud storage and multi-cloud security have both been extensively researched, multi-cloud security has received less attention. We back the transition to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

Bibliography

1. Alexa Huth and James Cebula. "The Basics of Cloud Computing".
2. Introduction to cloud computing by Dialogic.com.
3. appengine.google.com, developer.google.com.
4. Borko Furht Armando Escalante. "Handbook of Cloud Computing". by Springer.
5. G Juve., *et al*. "Scientific Workflow Applications on Amazon EC2". Workshop on Cloud-based Services and Applications in conjunction with 5th IEEE International Conference on e-Science (e-Science 2009), (2009).
6. Charles Severance. "Using Google App Engine-O'Reilly".
7. Rabi Prasad Padhy., *et al*. "X-as-a-Service: Cloud Computing with Google App Engine, Amazon Web Services, Microsoft Azure, and Force.com".
8. Ashraf Zia. "Identifying Key Challenges in Performance Issues in Cloud Computing".
9. Randy Marchany. "Cloud Computing Security Issues".
10. Albert Greenberg., *et al*. "The Cost of a Cloud: Research Problems in Data Center Networks".
11. Farhad Ahamed., *et al*. "Cloud Computing: Security and Reliability Issues".
12. Sahar Mohammad Abduljalil., *et al*. "A Novel Approach for Handling Security in Cloud Computing Services.
13. Joseph Yeruva MPHASIS. "SAP Cloud Computing".
14. Russell Craig., *et al*. "Cloud Computing in the Public Sector".
15. Moving from Legacy Systems to Cloud Computing: A Tata Communication White Paper.
16. GTSI Group. "Cloud Computing-Building a Framework for Successful Transition". White Paper, GTSI Corporation, (2009).
17. Rajnish Choubey., *et al*. "A Survey on Cloud Computing Security, Challenges and Threats". *International Journal on Computer Science and Engineering (IJCSE)* 3.3 (2011).
18. Andrew Joint and Edwin Baker. "Knowing the past to understand the present- issues in the contracting for cloud-based services". *Computer Law and Security Review* 27 (2011): 407-415.
19. Michael Miller. "Cloud Computing Pros and Cons for End Users". microsoftpartnercommunity.co.uk, (2009).
20. Radu Prodan and Simon Ostermann. "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers". 10th IEEE/ACM International Conference on Grid Computing, (2009).