2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

ENCRYPTEDAND EFFICIENT PRESERVING PROVABLE DATA POSSESSION IN CLOUD STORAGE

DEVASANI SHRAVANI[1] MR. B. RAJU[2]

[1] PG Student, Department of Computer Science and Engineering, Chaitanya institute of technology and science Kishanpura,Hanamkonda,Warangal -506001, (.TS).india

[2]Assistant Professor, Department of Computer Science and Engineering ,Chaitanya institute of technology and science kishanpura,Hanamkonda,Warangal -506001, (TS).india

[1]shravani.devasani@gmail.com, [2]braju1423@gmail.com

Abstract:

Secure and Efficient Privacy Preserving in Cloud Storage. Cloud computing is an emergent paradigm to provide reliable and resilient infrastructure enabling the users (data owners) to store their data and the data consumers (users) can access the data from cloud servers. This paradigm reduces storage and maintenance cost of the data owner. At the same time, the data owner loses the physical control and possession of data which leads to many security risks. Therefore, auditing service to check data integrity in the cloud is essential. This issue has become a challenge as the possession of data needs to be verified while maintaining the privacy. To address these issues this work proposes a secure and efficient privacy preserving provable data possession (SEPDP). Further, we extend SEPDP to support multiple owners, data dynamics and batch verification. The most attractive feature of this scheme is that the auditor can verify the possession of data with low computational overhead. Storage-as-a-service has emerged as a commercial alternative for local data storage due to its characteristics include less initial infrastructure setup, relief from maintenance overhead and universal access to the data irrespective of location and device. SEPDP: Secure and Efficient Privacy Preserving in Cloud Storage. Though it provides several benefits like cost saving, accessibility, usability, syncing and sharing, it raises several security threats as data is under the control of the cloud service provider (CSP). CSP can discard the rarely accessed data to save space and earn more profit, or it can lie about the data loss and data corruption, as a result of software/ hardware failure to protect its reputation. Therefore, it is necessary to check the possession of data in the cloud storage.In this paper, privacy preserving provable data possession scheme (named SEPDP) for untrusted and outsourced storage system is presented. Further, SEPDP is extended to support dynamic data updation by multiple owners and batch auditing. Security of the scheme is analyzed and showed that SEPDP protects data privacy from TPA while infeasible for CSP to forge the response without storing the appropriate blocks. SEPDP: Secure and Efficient Privacy Preserving in Cloud Storage. The most appealing features of the proposed scheme is to support all the important features including blockless verification, privacy preserving, batch auditing and data dynamics with lesser computation overhead.

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

I.INTRODUCTION

Storage-as-a-service has emerged as a commercial alternative for local data storage due to its characteristics include less initial infrastructure setup, relief from maintenance overhead and universal access to the data irrespective of location and device. Though it provides several benefits like cost saving, accessibility, usability, syncing and sharing, it raises several security threats as data is under the control of the cloud service provider (CSP). CSP can discard the rarely accessed data to save space and earn more profit, or it can lie about the data loss and data corruption, as a result of software/ hardware failure to protect its reputation. Therefore, it is necessary to check the possession of data in the cloud storage data generated from the wearable devices has high sampling rate and hence, it needs to be stored and handled carefully at the cloud centric data server. A wearable sensor based medical system includes various flexible sensors worn on various parts Identify applicable funding agency here. If none, delete this. of the body of a person (patient), including into textile fiber, clothes, elastic bands or even these can be directly Map reduce, great progress has also been made with hardware. Nowadays it is common for commodity clusters to have processors of more and more in-chip cores (referred to as many-core cluster hereafter. attached to the human body in case the devices are implantable medical devices. Traditional cryptographic solutions for integrity checking of data, either need a local copy of the data (which the data users (DUs) do not have) or allow the DUs to downloads the entire data. Neither of these solutions seems practical as earlier one requires extra storage and later alternative increases the file transfer cost. To address this issue, several schemes including are proposed which employ block less verification to verify the integrity without downloading the entire data. One of the attractive features of these works is to allow the public verifier to verify. With public auditability, DUs can recourse the auditing task to a third party auditor (TPA). It has expertise and capabilities to convince both the CSP These schemes use provable data possession (PDP) technique, which gives probabilistic data possession guarantee by randomly verifying few blocks for ensuring possession of data in the untrusted cloud storage. Privacy preserving is essential to prevent TPA to infer the data using the cloud servers response while auditing. However, the schemes proposed do not achieve privacy preserving requirement. Though data dynamics is an important feature to facilitate the data owners to insert, modify, and delete on a particular block of data, without changing the meta-data of other blocks, the techniques proposed in do not achieve data dynamics requirement. Meanwhile, the schemes like could not achieve batch auditing requirement which ensures that TPA should be capable enough to deal with the multiple numbers of simultaneous

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

verification requests from different DUs. This property is to save computation and communication.

II.EXISTING SYSTEM:

- PDP is introduced that uses random sampling of a few blocks for integrity verification.
- Shacham et al. designed two different integrity verification mechanisms. One uses pseudo-random function (PRF) which fails to provide public verifiability, while the other one uses boneh–lynn–shacham (BLS) signatures.
- Both the schemes support blockless verification but fail to provide privacy of the DO's data. Blockless verification requires linear combination of sampled blocks which gives a clue to TPA to extract the data.
- To preserve privacy of the data owner supporting blockless verification, Wang et al. proposed a public auditing scheme and extended that to support batch auditing further.

DISADVANTAGES OF EXISTING SYSTEM:

- Do not achieve privacy preserving requirement.
- Could not achieve batch auditing requirement which ensures that TPA should be capable enough to deal with the multiple numbers of simultaneous verification requests from different DUs
- Use pairing based cryptographic operations which are intensive computation and need more time.

III.PROPOSED SYSTEM:

- In this work, we propose a secure and efficient privacy preserving provable data possession scheme (SEPDP) for cloud storage. It operates in three phases, namely, key generation, signature generation and auditing phase.
- We extend SEPDP to support multiple data owners, batch auditing, and dynamic data operations. A probabilistic analysis to detect the integrity of the blocks stored at CSP.
- We evaluated the performance of the proposed scheme and compared with some of the existing popular mechanisms.

We observe that the total time for verification carried out by TPA in the proposed scheme is less than that of the existing schemes. This signifies that SEPDP is efficient and suitable to implement the verification at the low powered devices.

Architecture:

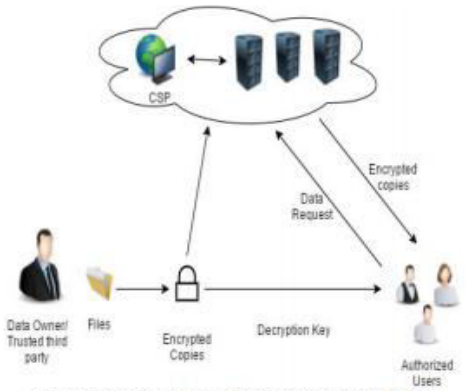

Fig. 1. Cloud Computing Data Storage System Model

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


Algorithm

TPA Auditing: The TPA Audit the data owner uploaded and downloaded file and file signature.A Third Party Administrator (TPA) is a service organization that provides a variety of services to the insurance industry in accordance with a service agreement. TPAs are usually utilized to provide services associated with employee benefits such as insurance related services to both insurance providers and companies that provide insurance to their employees.TPAs present a huge risk to user organizations (companies using a particular TPA) since TPAs may be processing millions of dollars worth of benefit claims for their clients. User organizations need assurance that the TPAs internal controls are designed and operating effectively to provide the outsourced benefit services. An independent audit of a TPA is one way to gain assurance regarding the TPAs internal control environment. TPA audits may include detailed tests of claims processed during a particular period of time, data analysis to identify trends and irregularities, and contract analysis. The TPA main goal is monitor the file database, uploaded and downloaded files. And receiver details auditing process. After receive the file is faced on block chain rule and it move on encrypted system The each block files are encrypted and stored on file databases for security purposed. If the client send the request for download the TPA audit the file name signature and username, e mail id and after it permit to download the particular file form database.

J. AES Encryption: The AES is Advanced Encryption Standard key is a Symmetric encryption key this is key is based on ANSCI code formation. This algorithm block key size is 128bit to 256bit. This cryptography is more secured. In our process the cloud data is secure encrypted at using AES encryption. After the encryption process is completed the AES key is generated.

IV.IMPLEMENATATION:

Data Owner:

Data owners are the entities who store their data in the cloud. DO share a secret key with TPA through a secure channel using any standard technique like SSL/TLS. Every block of the outsourced data is tagged with a signature computed using the private key of DO. We extend SEPDP to support multiple data owners. In Multiple data owner model in which each data owner has its own public key and private key. Each DO signs their corresponding data and stores both data and signatures in the CSP.

Data User:

Data users access and operate on those data kept at CSP. But, operating on the incorrect data leads to faulty result and create chaos which necessitate the integrity verification of remotely stored data. Data Users verification requests can be verified by the TPA.

Cloud Service Provider:

CSP is assumed to be semi-trusted. It executes the protocol without polluting data

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


integrity actively. At the same time, it may lie about the incorrectness of the data to save its reputation. Further, we consider that neither DU nor third party auditor is colluded with CSP to falsify the integrity check. CSP can pass the audit phase only if it possesses the outsourced data intact (same as uploaded by DO).

Third Party Auditor:

In the auditing phase, TPA sends a challenge to CSP and CSP returns a response to proof possession of the data. Thus, the public auditing schemes are a kind of challenge-response protocol. TPA should be capable enough to deal with the multiple numbers of verification requests from different DUs simultaneously. This feature saves both the computation cost of TPA as well as bandwidth consumption between CSP and TPA.

V.CONCLUSION:

In this paper, privacy preserving provable data possession scheme (named SEPDP) for untrusted and outsourced storage system is presented. Further, SEPDP is extended to support dynamic data updation by multiple owners and batch auditing. Security of the scheme is analyzed and showed that SEPDP protects data privacy from TPA while infeasible for CSP to forge the response without storing the appropriate blocks. The most appealing features of the proposed scheme is to support all the important features including blockless verification, privacy preserving, batch auditing and data dynamics with lesser computation overhead.

VI.REFERENCES:

[1] K. Yang and X. Jia, "Data storage auditing service in cloud computing: challenges, methods and opportunities," World Wide Web, vol. 15, no. 4, pp. 409–428, 2012.

[2] B. Wang, B. Li, H. Li, and F. Li, "Certificateless public auditing for data integrity in the cloud," in Proceedings IEEE Conference on Communications and Network Security (CNS), 2013, pp. 136–144.

[3] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proceedings of 14th ASIACRYPT, 2008, pp. 90–107.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proceedings of 29th IEEE Conference on Computer Communications (INFOCOM), 2010, pp. 1–9.

[5] L. Yuchuan, F. Shaojing, X. Ming, andW. Dongsheng, "Enable data dynamics for algebraic signatures based remote data possession checking in the cloud storage," China Communications, vol. 11, no. 11, pp. 114–124, 2014.

[6] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, 2015.

[7] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE

2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.