IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 08-10

Generating Unique Copies For Provable Multi-Copy Data Possession Scheme

[1]Sangavi. M ME-CSE PG STUDENT [2]V.Valarmathi (Associate Professor)
[3]T.Sathya (Assistant Professor)
Dept. Of Computer Science &Engg.
[1,2,3]Skr Engineering College, Agarmel, Chennai-600 123.

Abstract : *Increasingly more and more organizations are opting for outsourcing data to remote cloud service providers (CSPs). Customers can rent the CSPs storage infrastructure to store and retrieve almost unlimited amount of data by paying fees metered in gigabyte/month. For an increased level of scalability, availability, and durability, some customers may want their data to be replicated on multiple servers across multiple data centers.*

I Introduction

OUTSOURCING data to a remote cloud service provider (CSP) allows organizations to store more data on the CSP than on private computer systems. Such outsourcing of data storage enables organizations to concentrate on innovations and relieves the burden of constant server updates and other computing issues. Moreover, many authorized users can access the remotely stored data from different geographic locations making it more convenient for them. Once the data has been outsourced to a remote CSP which may not be trustworthy, the data owners lose the direct control over their sensitive data. This lack of control raises new formidable and challenging tasks related to data confidentiality and integrity protection in cloud computing. The confidentiality issue can be handled by encrypting sensitive data before outsourcing to remote servers. As such, it is a crucial demand of customers to have a strong evidence that the cloud servers still possess their data and it is not being tampered with or partially deleted over time. Consequently, many researchers have focused on the problem of provable data possession (PDP) and proposed different schemes to audit the data stored on remote servers. PDP is a technique for validating data integrity over remote servers. In a typical PDP model, the data owner generates some metadata/information for a data file to be used later for verification purposes through a challenge-response protocol with the remote/cloud server. The owner sends the file to be stored on a remote server which may be untrusted, and deletes the local copy of the file. As a proof that the server is still possessing the data file in its original form, it needs to correctly compute a response to a challenge vector sent from a verifier who can be the original data owner or a trusted entity that shares some information with the owner. Researchers have proposed different variations of PDP schemes under different cryptographic assumptions for example One of the core design principles of outsourcing data is to provide dynamic behavior of data for various applications. This means that the remotely stored data can be not only accessed by the authorized users, but also updated and scaled (through block level operations) by the data owner. PDP schemes presented in focus on only static or warehoused data, where the outsourced data is kept unchanged over remote servers. Examples of PDP constructions that deal with dynamic data are. The latter are however for a single copy of the datafile. Although PDP schemes have been presented for multiple copies of static data,, to the best of our knowledge, this work is the first PDP scheme directly dealing with multiple copies of dynamic data. In Appendix A, we provide a summary of related work. When verifying multiple data copies, the overall system integrity check fails if there is one or more corrupted copies. To address this issue and recognize which copies have been corrupted, we discuss a slight modification to be applied to the proposed scheme.

II Existing System

- Once the data has been outsourced to a remote CSP which may not be trustworthy, the data owners lose the direct control over their sensitive data. This lack of control raises new formidable and challenging tasks related to data confidentiality and integrity protection in cloud computing. The confidentiality issue can be handled by encrypting sensitive data before outsourcing to remote servers. As such, it is a crucial demand of customers to have a strong evidence that the cloud servers still possess their data and it is not being tampered with or partially deleted over time. Consequently, many researchers have focused on the problem of provable data possession (PDP) and proposed different schemes to audit the data stored on remote servers.
- One of the core design principles of outsourcing data is to provide dynamic behavior of data for various applications. This means that the remotely stored data can be not only accessed by the authorized users, but also

updated and scaled (through block level operations) by the data owner. PDP schemes presented focus on only static or warehoused data, where the outsourced data is kept unchanged over remote servers. Examples of PDP constructions that deal with dynamic data. The latter are however for a single copy of the data file.

DISADVANTAGE IN EXISTING SYSTEM

Once the data has been outsourced to a remote CSP which may not be trustworthy, the data owners lose the direct control over their sensitive data. This lack of control raises new formidable and challenging tasks related to data confidentiality and integrity protection in cloud computing..

III Proposed System

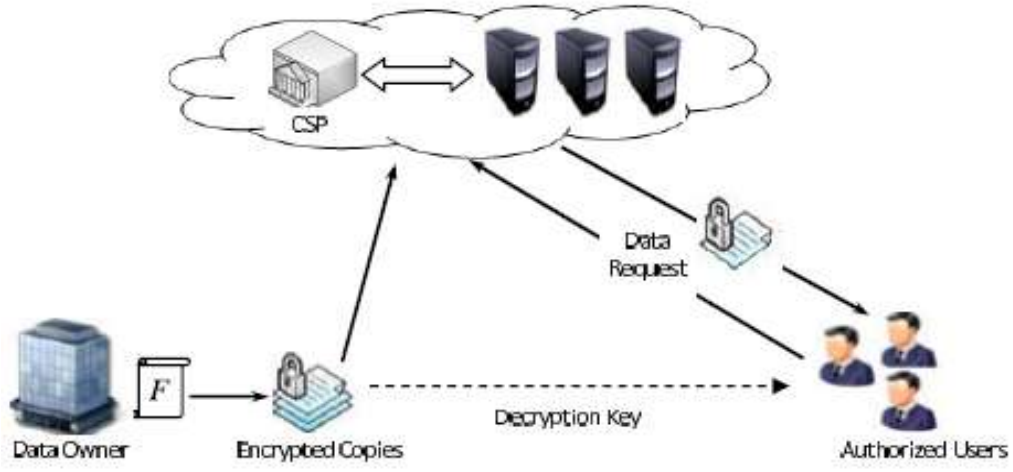
- When verifying multiple data copies, the overall system integrity check fails if there is one or more corrupted copies. To address this issue and recognize which copies have been corrupted, we discuss a slight modification to be applied to the proposed scheme. We propose a map-based provable multi-copy dynamic data possession (MB-PMDDP) scheme. This scheme provides an adequate guarantee that the CSP stores all copies that are agreed upon in the service contract. Moreover, the scheme supports outsourcing of dynamic data, i.e., it supports block-level operations such as block modification, insertion, deletion, and append. The authorized users, who have the right to access the owner's file, can seamlessly access the copies received from the CSP.
- We give a thorough comparison of MB-PMDDP with a reference scheme, which one can obtain by extending existing PDP models for dynamic single-copy data.
- We show the security of our scheme against colluding servers, and discuss a slight modification of the proposed scheme to identify corrupted copies.
- In this work, we do not encode the data to be outsourced for the following reasons. First, we are dealing with dynamic data, and hence if the data file is encoded before outsourcing, modifying a portion of the file requires re-encoding the data file which may not be acceptable in practical applications due to high computation overhead.
- Second, we are considering economically-motivated CSPs that may attempt to use less storage than required by the service contract through deletion of a few copies of the file. The CSPs have almost no financial benefit by deleting only a small portion of a copy of the file.
- Third, and more importantly, unlike erasure codes, duplicating data files across multiple servers achieves scalability which is a fundamental customer requirement in CC systems. A file that is duplicated and stored strategically on multiple servers – located at various geographic locations

ADVANTAGES OF PROPOSED SYSTEM:

Although PDP schemes have been presented for multiple copies of staticData, to the best of our knowledge, this work is the first PDP scheme directly dealing with multiple copies of dynamic data.

The storage model used in this work can be adopted by many practical applications. For example, e-Health applications can be envisioned by this model where the patients' database that contains large and sensitive information can be stored on the cloud servers. In these types of applications, the e-Health organization can be considered as the data owner, and the physicians as the authorized users who have the right to access, scientific, and educational applications can be viewed in similar settings.

IV Architecture Diagram



V Conclusion

Outsourcing data to remote servers has become a growing trend for many organizations to alleviate the burden of local data storage and maintenance. In this work we have studied the problem of creating multiple copies of dynamic data file and verifying those copies stored on untrusted cloud servers. We have proposed a new PDP scheme (referred to as MB-PMDDP), which supports outsourcing of multi-copy dynamic data, where the data owner is capable of not only archiving and accessing the data copies stored by the CSP, but also updating and scaling these copies on the remote servers. To the best of our knowledge, the proposed scheme is the first to address multiple copies of dynamic data. The interaction between the authorized users and the CSP is considered in our scheme, where the authorized users can seamlessly access a data copy received from the CSP using a single secret key shared with the data owner. Moreover, the proposed scheme supports public verfiability, enables arbitrary number of auditing, and allows possession-free verification where the verifier has the ability to verify the data integrity even though he neither possesses nor retrieves the file blocks from the server. Through performance analysis and experimental results, we have demonstrated that the proposed MB-PMDDP scheme outperforms the TB-PMDDP approach derived from a class of dynamic single-copy PDP models. The TB-PMDDP leads to high storage overhead on the remote servers and high computations on both the CSP and the verifier sides. The MB-PMDDP scheme significantly reduces the computation time during the challenge-response phase which makes it more practical for applications where a large number of verifiers are connected to the CSP causing a huge computation overhead on the servers. Besides, it has lower storage overhead on the CSP, and thus reduces the fees paid by the cloud customers. The dynamic block operations of the map-based approach are done with less communication cost than that of the tree-based approach. A slight modification can be done on the proposed scheme to support the feature of identifying the indices of corrupted copies. The corrupted data copy can be reconstructed even from a complete damage using duplicated copies on other servers. Through security analysis, we have shown that the proposed scheme is provably secure.

References

[1]. Amazon EC2 - Virtual Server Hosting
[2]. Yan-Cheng Chang Harvard University, New York, NY.
[3]. privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability Z. Hao, S. Zhong, and N. Yu.
[4]. On Verifying Dynamic Multiple Data Copies over Cloud Servers, Ayad F.Barsoum and M. Anwar Hasan
[5]. Provable Possession and Replication of Data over Cloud Servers,Ayad F.Barsoum and M.Anwar Hasan
[6]. A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability, Z. Hao ; Dept. of Electron. Eng. & Inf. Sci., Univ. of Sci. & Technol. of China, Hefei, China ; N. Yu