ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Survey of Integrity Verification in Cloud-Storage Using Various Techniques

Sheela.K, Sivasri.S

Dept. of I.T (IV year), IFET College of Engineering, Villupuram, TamilNadu, India

ABSTRACT: In cloud computing, an enormous amount of data is stored every day. Many organizations are now migrated to cloud and demand for resource is growing. Hence the providers are now delivering multi-cloud environment to meet this demand. If multiple providers cooperatively work together the availability of resource can be improved. But still clients are worrying that their data is properly stored and maintained by providers without intact. Though the providers are provide enough security there are still many security issues happening in cloud. This survey paper presents integrity verification of client data using various techniques.

KEYWORDS: Integrity verification, multi cloud, Provable Data Possession, Proofs of Retrievability, Identity Based Provable Data Possession

I. INTRODUCTION

Cloud computing is a large group of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud computing is a trend in the present day scenario with almost all the organizations are incoming into it. Cloud computing used virtualization concept and provide service based on "pay only for use" policy.**Pay-as-you-go –** Cloud computing will require a basic startup cost followed by a monthly usage charge but it cost lower than installing On-site file management. User company charge based on time spending and working in cloud.

II. LITERATURE SURVEY

In [1] authors introduced a model for provable data possession (PDP) that allows a client that has outsourced data at an untrusted cloud to verify that the server possesses the original data without downloading it. This model generates a probabilistic proof of possession through sampling random set of blocks from the server, which significantly reduces cost. The data owner maintains a constant amount of data to verify the proof. The request/response protocol transmits a little, constant amount of data, which reduces network communication. Thus, the Provable Data Possession model for remote data integrity checking supports the large data sets in widely-distributed storage system. The key component of this scheme is the homomorphic verifiable tags. In [2] authors introduced the efficient and secured outsourced data is addressed either by public key cryptography or requiring the user to outsource its data in encrypted form called EPDP (Efficient-PDP). This technique is based entirely on symmetric key cryptography and not requiring any bulk encryption. It allows dynamic data that efficiently support operations, such as block modification, deletion and append. Two different approaches PDP and POR have been proposed. The POR is a public key based technique allowing any verifier to query the server and obtain an interactive proof of data possession.In [3] authors proposed the POR scheme permits back-up service toproduces a concise proof that a client can retrieve a file F, that is, that the archive retains and reliably transmits file data sufficient for the user to recover F in its whole. A POR is a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file F. To explore POR protocols, in which the communication expenses, memory accesses for the proven, and storage necessities of the client are small parameters essentially independent of the length of F. The goal of a POR is to accomplish these checks without client having to retrieve the files themselves. A POR can also provide service with quality assurances.

In [4] authors introduced the problem of ensuring the integrity of data storage. In particular, to consider the task of allowing a third party auditor (TPA), on behalf of the user, to verify the integrity of the dynamic data stored in the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

cloud server. The introduction of TPA reduces the participation of the client through the auditing of whether their data in the cloud is indeed intact, which can be important in achieving financial system of scale for Cloud Computing.The operation supported by data dynamics such as block insertion and deletion, is also a major step toward practicality, services present in Cloud Computing are not limited to archive or backing data only. Earlier works on make confident of the remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. Initially identify the complexities and security problems of direct extensions with fully dynamic data operations from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in this protocol design.

This scheme achieves an efficient data dynamics, can develop the existing proof of storage models by manipulating the classic (MHT) Merkle Hash Tree structure for block tag authentication. To support efficient handling of severalauditing tasks, can further explore the technique of bilinear aggregate signature to extend a main result into a multiple user setting, where TPA can perform several auditing tasks concurrently.In [5] authors proposed security solutions based upon many aspects of a large and loosely integrated system. A data integrity checking protocol which eliminates the third party verifying, is explained to protect static data and dynamic data from unauthorized user, modification, or interference. There are some different definitions of cloud computing, but all of them agree on how to provide services to users of the network. Cloud computing is an Internet-based development and use of computer technology. It refers to the use of computing resources; hardware and software, available on demand as a service over the Internet. It offers a range of services for users of the network, which include applications, storage, and various operations etc.

In [6] authors considered the cloud data storage protection, which has always been an essential aspect of ensures the accuracy of client data in the cloud, it is denoting ineffective and flexible distributed verification scheme with two features. By utilizing the homomorphism token withflexible distributed verification achieves the storage correctness and data error localization. Unlike the most prior works, this scheme further supports secured and efficient dynamic operationson data blocks, including: data insert, update, delete and append. If supposed to find fraud in our outsourced data (e.g., when a server crashes or is compromised) in the storage cloud, then we should correct the corrupted data and restore the original data in the cloud.In [7] authors improved the Remote data integrity checking can make the client to verify their outsourced data is kept intact without retrieving the entire data. In some application scenarios, the users have to store their data on multi-cloud environment. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. Concrete ID-DPDP protocol is designed based on the bilinear pairing. The ID-DPDP protocol is provably secure under the hardness assumption of the standardCDH(computational DiffieHellman) problem. ID-DPDP protocol is also efficient and flexible because it eliminates the certificate management. Based on the client's authentication, the ID-DPDP protocol can realize private verification, delegated verification and open verification.

In [8] authors proposed Provable data possession (PDP) is a method for ensuring the integrity of data in cloud. In this paper, to address the construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration, in which to consider the presence of multiple cloud service providers to cooperatively store and maintain the clients' data. To present a cooperative PDP (CPDP) scheme based on homomorphic verifiable reaction and hash index hierarchy. Prove the security of the scheme based on multi-prover zero-knowledge proof system, which can fulfill completeness, information soundness, and zero-knowledge goods. In addition, articulate performance optimization mechanisms for this scheme, and in particular present an effective method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. This experiments show that our solution presents lesser computation and communication expenses in comparison with non-cooperative approaches. Cooperative PDP (CPDP) schemes accepting zero-knowledge property and three-layered index hierarchy, respectively. In particular effective method for choosing the optimal amount of sectors in each block to minimize the computation charges of clients and storage service providers. Cooperative PDP (CPDP) scheme without compromising data secrecy based on current cryptographic techniques.

In [9] authors proposed about cloud storage, users can remotely store their client data and appreciate the on-demand high-quality presentations and services from a shared pool of configurable computing assets, without the load of native

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

data storage and protection. The statement that client no larger have physical ownership of the uploaded data makes the data integrity security in cloud computing a difficult task, especially for clients with controlled computing assets. Moreover, users should be able to use the cloud storage as if it is resident, without distressing about the need to check its integrity. Thus, permitting open auditability for cloud storage is of serious importance so that client can resort to a third-party auditor to verify the integrity of outsourced data and free. To strongly introduce an effective TPA, the checking process should bring in no new weaknesses toward client data privacy, and present no supplementary online burden to user. In this paper, tointroduce a secure cloud storage structure supporting privacy-preserving public auditing. To further range this result to enable the TPA to perform verify for multiple users concurrently and powerfully. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

III. CONCLUSION AND FUTURE WORK

Cloud is designed to provide a service to the external users. To compensate their needs the resources should be highly available. In this survey, it gives overview about various integrity verification techniques. In addition, comparative study integrity verification schemes and its methodology are classified along with their adaptation to single/multi cloud environment. Using Distributed Storage Integrity Auditing mechanism verifies their client data in multi-cloud storage and also identifies the malicious cloud server and corrects it.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,D. Song, "Provable Data Possession at Untrusted Stores", *CCS'07*, pp.598-609, 2007
[2] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable andEfficient Provable Data Possession", *SecureComm 2008*, 2008.
[3]A. Juels, B. S. Kaliski Jr., "PORs: Proofs of Retrievability for LargeFiles", *CCS'07*, pp. 584-597, 2007.
[4] Qian Wang, Cong Wang, Jin Li, Kui Ren and WenjingLou ," Enabling Public Auditing and Data Dynamics for Storage Security in Cloud Computing", 2009.
[5] Dr.NEDHAL A.AL-SAIYD, NADA SAIL,"Data Integrity in Cloud Computing Security",2013.
[6]K.Sunitha, V.Tejaswini, S.K.Prashanth,"Availability and Integrity of Data Storage in Cloud", 2013.
[7] Wang .h, "Identity Based Distributed Provable Data Possession in multi-cloud storage"-wanh .h, 2014.
[8] O. RahamathunisaBegam1 , T. Manjula2 , T. Bharath Manohar3 , B. Susrutha4," Cooperative Schedule Data Possession for Integrity Verification in Multi-Cloud Storage", 2013.
[9] Cong Wang, Sherman S.M.Chow,Qian Wang, Kui Ren, Wenjing Lou"Privacy Preserving Public Auditing for Secure Storage " 2011.

BIOGRAPHY

Sheela.K , Pursuing B.Tech Information Technology Department in IFET College of Engineering at villupuram. My area of interests are Computer Networks , Cloud Computing etc.

Sivasri.S, Pursuing B.Tech Information Technology Department in IFET College of Engineering at villupuram. My area of interests are operating systems, Networking, Cloud Computing etc.