INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 2 (2016) PAGES 730-733
RECEIVED : 22/03/2016. PUBLISHED : 29/03/2016
March 29, 2016

INTEGRITY CHECKING OF DATA IN CLOUD STORAGE

[1]Karthikeyan.M, [2]Sahayarose.S, [3]Pavithra.K, [4]Karuppannan.R, [5]Umapathy.M,
[1,2,3,4] Dept of computer science engg, The Kavery Engineering College, Mechari.
[5]Asst prof, Dept of computer science engg, The Kavery Engineering College, Mechari.

Abstract:

Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. Challenging problem of existing system and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. it choose a efficient principle of "coordinate matching" i.e., as many matches as possible, to capture the similarity between search query and data documents, and further use "inner product similarity" to quantitatively formalize such principle for similarity measurement. The first propose a basic scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

Keywords: Cloud computing, integrity, multi cloud, data possession.

1. INTRODUCTION

Cloud computing has become an important theme in the computer field. Essentially, it takes the information processing as a service, such as storage, computing. It relieves of the burden for storage management, universal data access with independent geographical locations. At the same time, it avoids of capital expenditure on hardware, software, and personnel maintenances, etc. Thus, cloud computing attracts more intention from the enterprise. The foundations of cloud computing lie in the outsourcing of computing tasks to the third party. It entails the security risks in terms of confidentiality, integrity and availability of data and service. The issue to convince the cloud clients that their data are kept intact is especially vital since the clients do not store these data locally. Remote data integrity checking is a primitive to address this issue. For the general case, when the client stores his data on multi cloud servers, the distributed storage and integrity checking are indispensable. On the other hand, the integrity checking protocol must be efficient in order to make it suitable for capacity limited end devices. Thus, based on distributed computation, we will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi-cloud storage.

Multi cloud storage

Distributed computing is used to refer to any large collaboration in which many individual personal computer owners allow some of their computer's processing time to be put at the service of a large problem. In our system the each cloud admin consist of data blocks. The cloud user uploads the data into

multi cloud. Cloud computing environment is constructed based on open architectures and interfaces; it has the capability to incorporate multiple
internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud .A multi-cloud allows clients to easily access his/her resources remotely through interfaces.

Cooperative PDP

Cooperative PDP (CPDP) schemes adopting zero-knowledge property and three-layered index hierarchy, respectively. In particular efficient method for selecting the optimal number of sectors in each block to minimize the computation costs of clients and storage service providers. Cooperative PDP (CPDP) scheme without compromising data privacy based on modern cryptographic techniques.

Data Integrity

Data Integrity is very important in database operations in particular and Data warehousing and Business intelligence in general. Because Data Integrity ensured that data is of high quality, correct, consistent and accessible.

Third Party Auditor

Trusted Third Party (TTP) who is trusted to store verification parameters and offer public query services for these parameters. In our system the Trusted Third Party, view the user data blocks and uploaded to the distributed cloud. In distributed cloud environment each cloud has user data blocks. If any modification tried by cloud owner a alert is send to the Trusted Third Party.

Cloud User

The Cloud User who has a large amount of data to be stored in multiple clouds and have the permissions to access and manipulate stored data. The User's Data is converted into data blocks. The data blocks are uploaded to the cloud. The TPA views the data blocks and Uploaded in multi cloud. The user can update the uploaded data. If the user wants to download their files, the data's in multi cloud is integrated and downloaded.

2. RELATED WORK

In cloud computing, remote data truthfulness checking is an important security problem. The clients' massive data is outside his control. The malicious cloud server may corrupt the clients' data in order to gain more benefits. Many researchers proposed the analogous system model and security model. In 2007, provable data possession (PDP) paradigm was proposed by Atenieseet al.[1].In the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA they designed two provably secure PDP schemes. After that, Ateniese et al. proposed dynamic PDP model and concrete scheme [2] although it does not support insert operation. In order to prop up the insert operation, in 2009, Erway et al. proposed a full-dynamic PDP scheme based on the genuine flip table [3]. The similar work has also been done by F. Sebéet al. [4]. PDP allows a verifier to verify the remote data reliability without retrieving or downloading the whole data. It is a probabilistic proof of ownership by sampling random set of blocks from the server which drastically reduces I/O costs. The verifier only maintains small metadata to perform the integrity checking. PDP is an

interesting remote data integrity checking model. In 2012, Wang projected the security model and concrete scheme of proxy PDP in public clouds [5]. At the same time, Zhu et al. proposed the cooperative PDP in the multicloud storage [6].

3. PROPOSED SYSTEM

We define and solve the challenging problem of existing system, and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching. We first propose a basic scheme using secure inner product computation, and then significantly improve it to meet different privacy requirements in two levels of threat models. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given, and experiments on the real-world dataset further show proposed schemes indeed introduce low overhead on computation and communication.

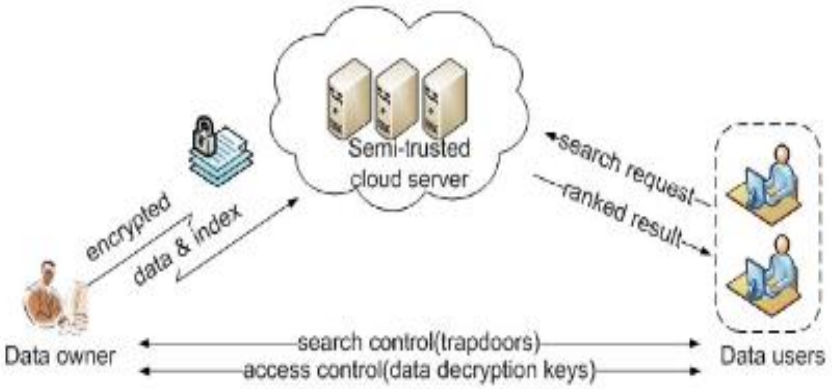

Fig.1. Architecture of the search over encrypted cloud data

Multi keyword ranked search over encrypted cloud data, and establish a set of strict privacy requirements for such a secure cloud data utilization system.

CONCLUSION

In multi cloud storage, this paper formalizes the ID-DPDP system model and security model. At the same time the first ID-DPDP protocol which is provably secure under the assumption that the CDH problem is hard. Besides of the elimination of certificate management. Our ID-DPDP protocol has also flexibility and high efficiency. At the same time the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification based on the client's authorization.

FUTURE WORK

The over encrypted cloud data and establish a variety of privacy requirements. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching" i.e. as many matches as possible to effectively capture the relevance of outsourced documents to the query keywords and use "inner product similarity" to quantitatively evaluate such similarity measure.

REFERENCES

[1] G.Ateniese,R.Burns,R.Curtmola,J.Herring,L.Kissner, Z. Peterson, and D. Song, ‘‘Provable Data Possession at Untrusted Stores,’’ in Proc. CCS , 2007, pp. 598-609.

[2] G. Ateniese, R. DiPietro, L.V. Mancini, and G. Tsudik, ‘‘Scalable and Efficient Provable Data Possession,’’ in Proc. SecureComm ,2008, pp. 1-10.

[3] C.C.Erway,A.Kupcu,C.Papamanthou,andR.Tamassia, ‘‘Dynamic Provable Data Possession,’’ in Proc. CCS , 2009,pp. 213-222.

[4]F. Sebé ,J.Domingo-Ferrer,A.Martínez-Balleste ,Y.Deswarte, and J. Quisquater, ‘‘Efficient Remote Data Integrity Checking in Critical Information Infrastructures,’’ IEEE Trans. Knowl. Data Eng. , vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[5] H.Q. Wang. (2013, Oct./Dec.). Proxy Provable Data Possession in Public Clouds. IEEE Trans. Serv. Comput. [Online].6(4),pp. 551-559.
Available: http://doi.ieeecomputersociety.org/10.1109/TSC.2012.35

[6] Y. Zhu, H. Hu, G.J. Ahn, and M. Yu, ‘‘Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage,’’ IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

AUTHORS

Umapathy.M, Asst prof, Dept of computer science engg, The Kavery Engineering College, Mechari.

Karthikeyan.M, Dept of computer science Engg, The Kavery Engineering College Mechari.

Pavithra.K, Dept of computer science Engg, The Kavery Engineering College, Mechari.

Sahayarose.S, Dept of computer science Engg, The Kavery Engineering College, Mechari.