International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

Enhancement of Decryption Operation for Resource Limited Devices

M.UmaMaheswara Rao[1] & Dr. M. Babu Rao[2]

1M-Tech Dept. C.S.E, Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh 521356, India Mail Id: - umamahesh.mtech22@gmail.com

[2]Professor& HOD of Dept. CSE, Gudlavalleru Engineering College, Gudlavalleru, Andhra Pradesh 521356, India Mail Id: - baburaompd@gmail.com

Abstract

In recent years, cloud storage accommodation has become a more expeditious profit magnification by providing its features for client's data. Privacy preservation and data integrity are the two main issues faced by single cloud accommodation providers. Hence distributed cloud environment, multi cloud is utilized. In the subsisting system, when client shops his information on multi-cloud servers, ye distributed store plus integrity checking are in peril. Provable data possession is a method for ascertaining the integrity of data in storage outsourcing. The proposed ID-DPDP protocol able to provide client's identity with his private key and provably secure under the hardness postulation of the standard CDH quandary.. It will check clients data kept safely without downloading the whole data. This protocol eliminates certificate management, efficient and flexible.

Keywords: Cloud Computing, Multi Cloud, Provable Data Possession, Data Integrity Checking.

1. Introduction

In recent years, cloud storage accommodation has become a more expeditious profit magnification point by providing a commensurably low-cost, scalable, position-independent platform for clients' data. Since cloud computing environment is constructed predicated on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud accommodations together to provide high interoperability. We call such a distributed cloud environment as a multi-Cloud (or hybrid cloud). Often, by utilizing virtual infrastructure management (VIM) , a multi-cloud sanctions clients to facilely access his/her imaginations remotely by interfaces such as Web accommodations provided by Amazon EC2. There subsist sundry implements and technologies for multicloud, such as Platform VM Orchestrator, VMware

vSphere, and Ovirt. These implements avail cloud providers construct a distributed cloud storage platform (DCSP) for managing clients' data. However, if such a consequential platform is vulnerably susceptible to security attacks, it would bring irretrievable losses to the clients.

For example, the confidential data in an enterprise may be illicitly accessed through a remote interface provided by a multi-cloud, or germane data and archives may be disoriented or tampered with when they are stored into a dubious storage pool outside the enterprise. Therefore, it is indispensable for cloud accommodation providers (CSPs) to supply surety techniques for dealing their storage accommodations. Provable data possession (PDP) (or proofs of recoverable (POR) is this a probabilistic validation technique for a storage provider to prove the integrity and ownership of clients' information without downloading information. The proof-checking without downloading makes it especially paramount for immensely colossal-size files and folders (typically including many clients' files) to check whether these data have been tampered with or expunged without downloading the latest version ofdata. Thus, it is able to supersede traditionalistic hash and signature operates in storage outsourcing. Sundry PDP schemes have been recently proposed, such as Scalable PDP plus Dynamic PDP. However,these schemes mainly fixate on PDP issues at untrusted servers in a single cloud storage provider and are not felicitous for a multi-cloud environment.

2. Related Work

Existing System:

Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys. Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. Hanaoka et al. proposed a way for users to periodically renew their private keys without interacting with PKG. Lin et al. proposed a space efficient revocable IBE mechanism from non-monotonic Attribute-Based Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where the number of revoked users is.

Disadvantages of existing system:

- Boneh and Franklin mechanism would result in an overhead load at PKG. In

another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows.

- Boneh and Franklin's suggestion is more a viable solution but impractical.
- In Hanaoka et al system, however, the assumption required in their work is that each user needs to possess a tamper-resistant hardware device.
- If an identity is revoked then the mediator is instructed to stop helping the user. Obviously, it is impractical since all users are unable to decrypt on their own and they need to communicate with mediator for each decryption.

PROPOSED SYSTEM:

In this paper, we introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. We propose a scheme to offload all the key generation related operations during key-issuing and keyupdate, leaving only a constant number of simple operations for PKG and eligible users to perform locally. In our scheme, as with the suggestion, we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decryptability, unrevoked users needs to periodically request on keyupdate for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP).

Advantages of proposed system:

- Compared with the previous work, our scheme does not have to re-issue the whole private keys, but just need to update a lightweight component of it at a specialized entity KU-CSP.
- We also specify that

- with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKGis allowed to be offline after sending the revocation list to KU-CSP.
- No secure channel or user authentication is required during key-update between user and KU-CSP.
- Furthermore, we consider to realize revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model.
- Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

3. Implementation

The ID-DPDP system model and security definition are presented in this section. An ID-DPDP protocol constitutes four different entities which are illustrated in Fig 3. Described as below:

(i) Client: an entity, which has massive data to be stored on the multi-cloud for maintenance and computation, can be either single user or corporation.

(ii)CS (Cloud Server): an entity, which is managed by cloud service provider, has substantial storage place plus computation resource to maintain the clients' data.

(iii)Combiner: an entity, which gets the storage petition and disseminates the block-tag pairs to the corresponding cloud servers. When receiving the challenge, it splits the challenge plus disseminates them to the different cloud servers. Whenreceiving the responses from the cloud servers, it mixes them plus sends out the combined response to the verifier.

(iv)**PKG (Private Key Generator):** an entity, when getting the identity, it outputs the representing private key

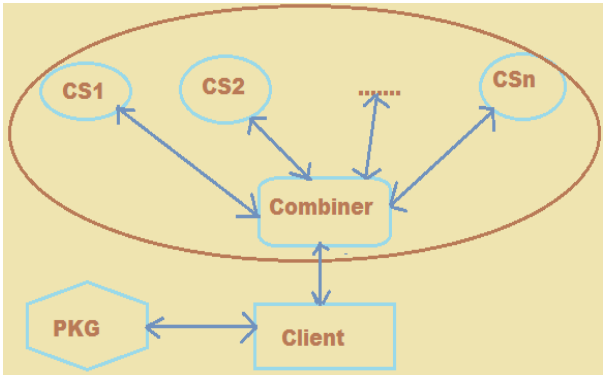

Fig 1:ID-DPDP Architecture

This protocol constitutes four procedures: Setup, Extract, TagGen, and Proof. The fig.1 can be described as follows:

1. In the phase Extract, PKG engenders the private key for the client.

2. The client engenders the block-tag pair and uploads it to mix. The combiner disseminates the block-tag pairs to the different cloud servers according to the storage metadata.

3. The verifier sends the challenge to combiner and the combiner distributes the challenge query to the representing cloud servers granting to the storage information.

4. The cloud servers respond the challenge and the combiner aggregates these replications from the cloud servers. The combiner sends the aggregated replication to the verifier. Determinately, the verifier checks whether the aggregated replication is valid. The concrete ID-DPDP construction mainly emanates from the signature, provable data possession and distributed computing. The signature relates the client's identity with his secret key. Distributed calculating is utilized to store the client's data on multi-cloud servers. Concurrently, distributed computing is withal used to coalesce the multi-cloud servers' replications to respond the verifier's challenge. Predicated on the provable data possession protocol, the ID-DPDP protocol is constructed by making utilization of the signature and distributed computing.

4. Experimental Work

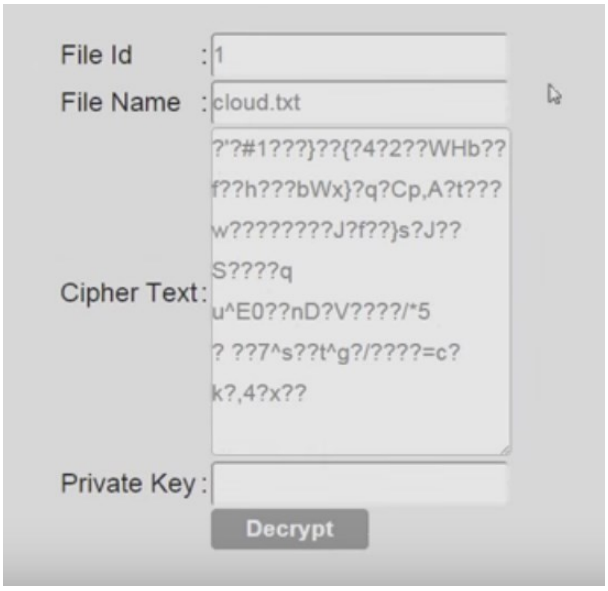

Fig 2: File Upload with Encryption.

Fig 3: Out Sourced Data

5. Conclusion

This paper formalizes the ID-DPDP system model and security model. ID-DPDP protocol works efficiently in multi cloud environment. Besides of the elimination of certificate management, our ID-DPDP protocol has additionally flexibility and high efficiency. Concurrently, the proposed ID-DPDP protocol can realize private verification, delegated

verification and public verification predicated on the client's sanction.

6. References

[1] P. Mell and T. Grance, "Draft nist working definition of cloud computing," Referenced on June. 3rd, 2009.

[2] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", SecureComm 2008, 2008.

[3] 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.

[4] C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "DynamicProvable Data Possession", CCS'09, pp. 213-222, 2009.

[5] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J.Quisquater, "Efficient Remote Data Integrity checking in Critical InformationInfrastructures", IEEE Transactions on Knowledge and DataEngineering, 20(8), pp. 1-6, 2008.

[6] H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012.

[7] Y. Zhu, H. Hu, G.J. Ahn, M. Yu, "Cooperative Provable Data Possessionfor Integrity Verification in Multicloud Storage", IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2231-2244, 2012.

[8] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", CCS'10, pp. 756-758, 2010.

[9] R. Curtmola, O. Khan, R. Burns, G. Ateniese, "MRPDP: Multiple-Replica Provable Data Possession", ICDCS'08, pp. 411-420, 2008.

[10] A. F. Barsoum, M. A. Hasan, "Provable Possessionand Replication of Data over Cloud Servers", CACR,University of Waterloo, Report2010/32,2010.