Scope International Journal of Science, Humanities, Management and Technology. ISSN : 2455-068X
Vol.2 Issue 4 (2016) 7 - 11. Submitted 29/10/2016. Published 12/11/2016

CLOUD COMPUTING BASED PRIVACY-PRESERVING AUTHENTICATION PROTOCOL IN SHARED AUTHORITY

[1]S.P.Madhumitha, [2]R.Radha,
[1]M.Phil Scholar, Dept of Computer Science, Bharathiyar Arts and Science College for Women, Deviyakurichi,
[2]Assistant professor, Dept of Computer Science, Bharathiyar Arts and Science College for Women, Deviyakurichi.

Abstract:

Cloud computing is emerging as a prevalent data interactive prototype to realize user's data remotely stored in an online cloud server. Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing. In address the building of an efficient PDP scheme for distributed cloud storage to maintain the scalability of overhaul and data migration in which it consider the existence of various cloud service providers to cooperatively store and maintain the clients' information. It present a cooperative PDP (CPDP) scheme based on homomorphism confirmable response and hash index hierarchy. In this work, that has recognized a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access influence sharing. Authentication is conventional to guarantee data confidentiality and data integrity. Data ambiguity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to surreptitiously inform the cloud server about the users 'access desires. Forward security is realized by the conference identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

Keyword: Cloud computing, authentication protocol, privacy preservation, shared authority.

1. INTRODUCTION

Cloud computing has received considerable concentration from both academic circles and industry due to a number of imperative advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, suppleness to scale up and down in sequence technology (IT) capacity and mobility where customers can access information wherever they are, rather than having to stay behind at their desks. Among various services of cloud computing, enabling secure access to outsourced data lays a solid foundation for information management and other operations. However, more research efforts are needed to achieve flexibly access control to large-scale dynamic data. For example, using asymmetric encryption to protect data or metadata will impact the adoption of the outsourcing display place by devices with limited computational power (e.g. mobile devices). At the same time, user-group-based information encryption may lead to a complicated access hierarchy after a series of grant and revocation operations.

2. RELATED WORK

In this paper [1] "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding" The main objective of this project is constructing a secure storage system with the intention of supports multiple functions is difficult when the storage system is disseminated and has no central authority. In this project we propose a threshold proxy re-encryption method and amalgamate it which a decentralized scoring through code such that a secure distributed storage system is formulated. In this

paper[2]" Enabling Public Audit ability and Data Dynamics for Storage Security in Cloud Computing" The main technical contribution is that the alternative re-encryption method supports encoding operations over encrypted messages as well as forwarding operations over encoded and encrypted messages. Our method completely integrates encrypting, encoding, and forwarding. These parameters allow more flexible modification between the number of storage servers and influence. Erasure encoding supports the forwarding scheme and applicable in decentralized distributed system. A decentralized erasure code is used to make certain the data robustness in the disseminated cloud storage organization. In erasure codes, the copy of the message is stored in the each storage servers.

In this paper [3] "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud" With the character of low maintenance cloud computing provides a cost-effective and efficient solution for sharing group supply among cloud users. Sharing data in a multi-owner manner while preserving data and identity privacy from an entrusted cloud is still a challenging issue, due to the frequent modify of the membership. In this paper, we propose a secure multi owner data sharing method named Mona for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile the storage space in the clouds and encryption computation cost of our scheme are self-governing with the number of revoke users. In addition we analyze the security of our method with rigorous proofs and demonstrate the efficiency of our scheme in experiments.

3. EXISTING SYSTEM

Despite the tremendous benefits outsourcing multiplication to the profitable public cloud is also depriving customer's direct control over the systems that consume and produce their data during the computation, which inevitably brings in new security concerns and challenges towards this talented computing model. On the one hand the outsourced computation workloads often contain sensitive information, such as the business financial records proprietary research data or personally identifiable health information sets. The unauthorized information leakage, sensitive data have to be encrypted previous to outsourcing. so as to provide end to- end data confidentiality assurance in the cloud and beyond. Unauthorized information leakage sensitive data have to be encrypted before outsourcing. So as to provide end to- end data confidentiality assurance in the cloud and beyond. For example, for the computations that require a large amount of computing resources, there are huge financial incentives for the cloud to be "lazy" if the customers cannot tell the correctness of the output. Besides, possible software bugs, hardware failures, or even outsider attacks might also affect the quality of the computed results.

Disadvantage

The cloud is intrinsically not secure from the viewpoint of customers without provided that a instrument for protected computation outsourcing so to protect the sensitive input and output information of the workloads. The various motivations for cloud server to execute unfaithfully and to return mistaken results i.e., they may behave beyond the classical semi hones model.

4. PROPOESD SYSTEM

Implementation is the stage of the project when the theoretical design is twisted out into a working system. Thus it can be deliberate to be the most critical stage in achieving a successful new system and in bountiful the user self-assurance that the new organization will work and be successful. The

accomplishment stage involves careful planning examination of the existing system and it's constraints on implementation designing of methods to achieve changeover and assessment of exchange methods.

Advantages

Confidentiality

- Outsourced data must be protected from the TTP the CSP and users that are not granted access.

Integrity

- Outsourced data are required to remain intact on cloud servers. The data owner and authorized users must be enabled to recognize data corruption over the CSP side.

Access control

- Only authorized users are allowed to access the outsourced data.

CSP's defense

- The CSP must be safeguarded against false accusations that may be claimed by dishonest owner/users, and such a malicious behavior is required to be revealed.

5. PROCESS

The abovementioned privacy issue to advocate a shared authority based privacy preserving authentication protocol (SAPA) for the cloud data storage which realizes authentication and agreement devoid of compromising a user's not to be mentioned information. The main donations are as follows.

- Identify a new privacy challenge in cloud storage and address a subtle privacy issue during a user challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access authority.
- Propose an authentication protocol to augment a user's access request related privacy and the shared access influence is achieved by anonymous access request matching mechanism.
- Apply cipher text-policy quality based access control to realize that a user can dependably access its own data fields and accept the proxy re-encryption to provide temp authorized data sharing among manifold users.

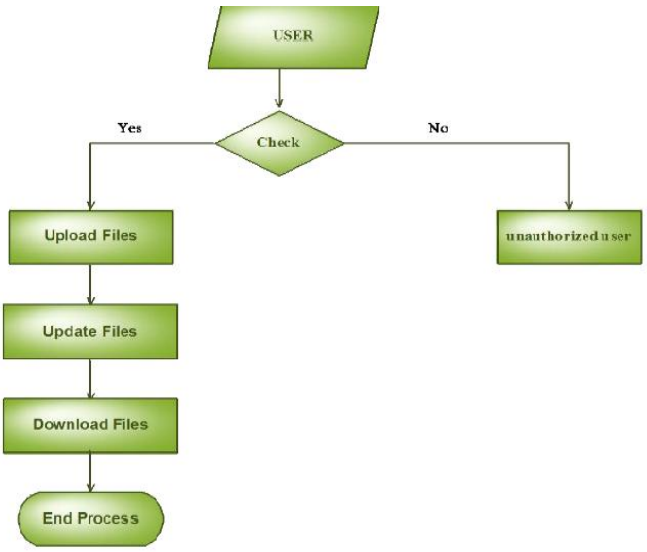

Fig.1. Cloud users

6. SYSTEM MODEL

To check the availability and integrity of outsourced data in cloud storages researchers have proposed two basic approaches called Provable Data Possession and Proofs of Irretrievability. First proposed the PDP model for ensuring control of files on untreated storages and provided an RSA based method for a static case that achieves the communiqué cost. They also proposed a in public confirmable version which allows anyone not just the owner to challenge the server for data ownership. They proposed a lightweight PDP scheme based on cryptographic hash function and symmetric key encryption but the servers can deceive the owners by using previous metadata or responses due to the lack of randomness in the challenges. The information of updates and challenges are incomplete and fixed in advance and users cannot execute block insertions anywhere.

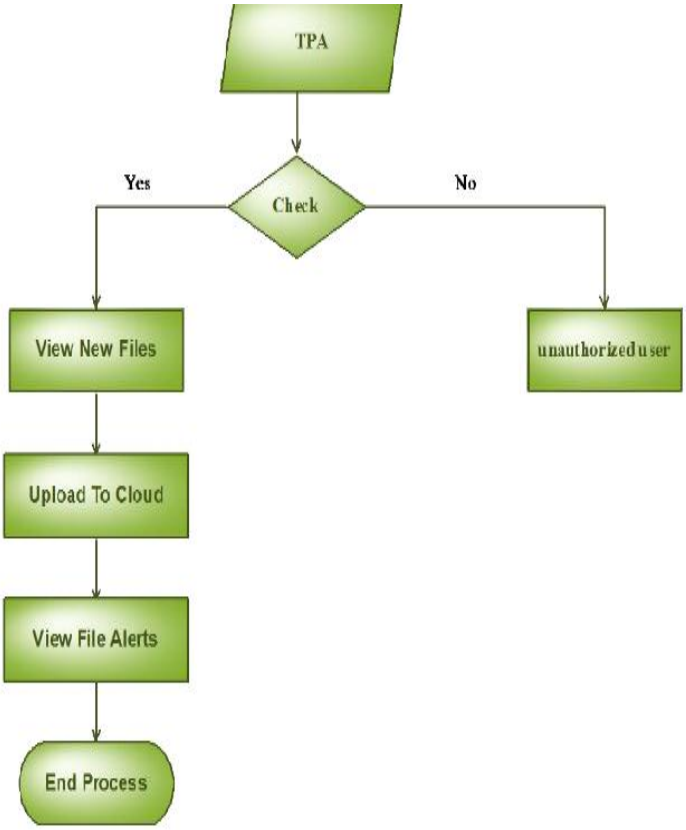

Fig.2. Trusted Third Party

The Cloud User who has a outsized amount of data to be stored in multiple clouds and encompass the permissions to access and stage-manage 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 requirements to download their files, the data's in multi cloud is included and downloaded. The Cloud User who has a outsized amount of data to be stored in multiple clouds and encompass the permissions to access and stage-manage 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 requirements to download their files, the data's in multi cloud is included and downloaded.

CONCLUTION

New privacy challenge during data accessing in the cloud computing to accomplish privacy-preserving access authority sharing. Authentications established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is improved by anonymous access requests to privately let somebody know the cloud server about the user's admittance desires. Forward security is realized by the session identifiers to avoid the session association. It indicates that the proposed scheme is possibly applied for enhanced space to yourself preservation in cloud applications.

REFERENCE

[1] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data EEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.

[2] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer , vol. 45, no. 7, pp. 73-78,2012.

[3] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no, 12, pp. 2231-2244, 2012

[4] A. Barsoum and A. Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Transactions on Parallel and Distributed Systems,Volume 8 No:2, November 2013.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th conference on Information communications, ser. INFOCOM'10. IEEE Press, 2010, pp. 534–542.