International Journal of Science Engineering and Advance Technology

Permitting Data Active For Cloud Processing Storage Method

M Anusha #1, P Naga Deepthi #2
#1Student of M.Tech (CSE) and Department of Computer Science Engineering,
#2 Asst.Prof, Department of Computer Science and Engineering, Sir C R Reddy College of Engineering, Eluru, W.G.DIST

Abstract:
Cloud service providers are having service metrics and service dimensions. With out these the cloud computing will not be executed. So we are providing saas , paas and iaas are providing for cloud with permitting data active for cloud processing storage methods. In current clouds are not understandable, not having integrity so previous clouds are manipulated. But now a days we are providing privatization for clouds. The cloud service providers are not understandable manner these are having so many risk like scalability and resourcability.
So the clouds are concentrated on mitigate these type of risks. But we did not solve purely so we are introducing present cloud infrastructure it will be solve the respected problems like access controllability, retivability, efficiency and migration of clouds.

Keywords: Access control, Cloud computing, Cloud service provider, Data security, Data outsourcing ,Mutual trust.

Introduction

Cloud computing capable technology for storage and communication with huge amount investment. cloud has plays attention on present business and educational ways. It is flexible technology for all the people in the world. cloud communication rather than having to remain at their levels. The current Cloud computing is a distributed computational model over a large pool of shared virtualized computing resources (e.g., Storage, processing power, memory, applications, services, and network bandwidth). Cloud service providers (CSPs) offer various metric classes of services (Storage as a Service (SaaS), Application as a Service, and Platform as
a Service) that allow organizations to concentrate on their core business and leave the IT operations to experts. In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. Therefore, Storage as a Service providing resource by cloud service providers (CSPs) pool as a solution to mitigate the emergency of huge local data storage and reduce the maintenance outlay by means of outsourcing data storage. Through subcontract data storage manner, data owners delegate the storage and management of their data to a CSP in exchange for presiding fees metered in GB/month cloud servers are enable and provide data to remotely the users. But in this type of view other cloud users access the sensitive information of other users. Moreover, cloud service providers have been remotely access and manipulate data of usage. But this is not acceptable manner so we are providing privileges to users and remote servers. . The confidentiality feature is surly by the owner via encrypting the data before outsourcing to remote servers. The proposed model provides reliable computing and address the failures remote and dynamic users and also servers. This means that the dynamic stored data should be accessed only prevailed person and should remain secrecy. The CSP needs to be safe keeping from any false accusation that may be claimed by a data.

Existing System

It is majorly concentrated on cheater's of cloud provider and owners of data . The CSP first verifies privatization of owner before storing data on cloud. cloud service providers have been remotely access and manipulate data of usage. But this is not acceptable manner so we are providing privileges to users and remote servers. In case of failed verification, the CSP rejects to store data and asks the owner to resend the correct privileges. If the privileges is valid, both the file and
signature are stored on the cloud servers. The digital owner to get illegal compensations. signature achieves non repudiation from the owner side.
When an authorized user (or the owner) requests to retrieve the data file, the CSP sends file, owner's signature and CSP's signature on (file || owner's signature). The authorized user first verifies the CSP's signature. In case
of failed verification, the user asks CSP to re perform the transmission process. If CSP's signature is valid, the user then verifies owner's signature. If verification fails, this indicates the corruption of data over the cloud servers. The CSP cannot repudiate such corruption for the owner's signature is previously verified and stored by the CSP along with file. Since CSP's signature is attached with the
received data, a dishonest owner cannot falsely accuse the CSP regarding data integrity. The above solution increases the storage overhead on

cloud as owner's signature is stored along with the file on cloud servers. Moreover, there is an increased computation overhead, CSP has to verify signature of owner before storing file on cloud, and the authorized user verifies two signatures for each received file. If the CSP receives file from trusted entity other than the owner, the signature verification is not needed since the trusted entity has no incentive for repudiation or collusion. Therefore, delegating small part of owner's work to the TTP reduces both the storage and computation overheads. However the outsourced data must be kept private and any leakage of data toward the TTP must be prevented Limitations

1.The CSP is untrusted, and thus the confidentiality and integrity of data in the cloud may be at risk.

2.Computation Overhead is more in owner side As well as CSP side

3.A data owner and authorized users may collude and falsely accuse the CSP to get a certain amount of reimbursement.

4.The Owner May Loss the direct control over the sensitive data.

propose a scheme that addresses important issues related to outsourcing the storage of data, namely dynamic data ,

Newness , mutual trust, and access control . The remotely stored data can be not only accessed by authorized users, but also updated and scaled by the owner. After updating, authorized users should receive the latest version of the data (newness property), i.e., a technique is required to detect whether the received data is stale. Mutual trust between the data owner and the CSP is another imperative issue, which is addressed in the proposed scheme.

A mechanism is introduced to determine the dishonest party, i.e., misbehavior from any side is detected and the responsible party is

identified. Last but not least, the access control is considered, which allows the owner to grant or revoke access rights to the outsourced

data.

Advantages Of Proposed System

- It allows a data owner to outsource the data to a CSP, and perform full dynamic operations at the block level, i.e., it supports operations such as block modification, insertion, deletion, and append;
- It ensures the newness property, i.e., the authorized users receive the most recent version of the outsourced data;
- It establishes indirect mutual trust between the data owner and the CSP since each party resides in a different trust domain; and
- It enforces the access control for the out sourced data.

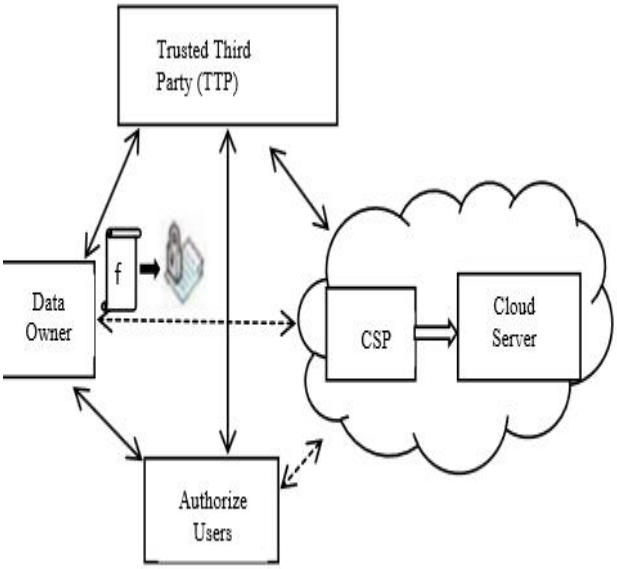

Figure.1 SystemArchitecture

Conclusion

In this paper, we have proposed a cloud based storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the CSP, but also updating and scaling this data on the remote servers. The proposed scheme enables the authorized users to ensure that

they are receiving the most recent version of the outsourced data. Moreover, in case of dispute regarding data integrity newness, a

TTP is able to determine the dishonest party. The data owner enforces access control for the outsourced data by combining three

cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme. The cloud based storage scheme is proposed that allows owner to benefit from facilities offered by the CSP and enables Detection of Dishonest entity (i.e. owner/CSP).It enables data owners to release their concerns regarding confidentiality, integrity, access control of the outsourced

data. To resolve disputes that may occur regarding data integrity, a trusted third party is invoked to determine the dishonest party (owner or CSP)

References

[1] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws.amazon.com, 2008.

[2] K. E. Fu, "Group sharing and random access in cryptographic storage file systems," Master's thesis, MIT, Tech. Rep., 1999.

[3] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage SLAs with cloud proof," in
Proceedings of the 2011 USENIX conference
, 2011.
[4] W. Wang, Z. Li, R. Owen s, and B. Bhargava, "Secure and efficient access to outsourced data," in Proceedings of the 2009 ACM workshop on Cloud computing security
, 2009, pp. 55 66.

[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted storage," in Proceedings of the FAST 03: File and Storage Technologies , 2003.

[6] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short cipher texts and private keys," in
Advances in Cryptology -CRYPTO, 2
005, pp. 258 275.

[7] F. Seb´e, J. Domingo Ferrer, A. Martinez Balleste, Y. Deswarte, and J.J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. And Data Eng., vol. 20, no. 8, 2008.

[8] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, 2008, pp. 1-10.