MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

ENABLING DYNAMIC DATA AND INDIRECT MUTUAL TRUST FOR STANDALONE STORAGE SYSTEM

Jayavant B. Somase, Om V. Kanade, Shivprasad R. Kankatte, Uddhav T. Kale

Department of Computer Engineering, JSPM's Imperial College Of Engineering & Research, Wagholi, *SavitribaiPhule Pune University, Pune*
jayavantsomase@gmail.com, omkanade123@gmail.com,
kankatte.shiv@gmail.com, utkale1991@gmail.com

Abstract: *Now a days, there are many organizations as well as individuals and they have an amount of sensitive data including personal information , some financial records , some important health records and such many more important information related to individual or any organization. That data produced by many organizations is out pacing their storage ability. Due to huge amount of data, it requires high storage capacity, so it is quite expensive. Hence, storage system offered by Standalone Service Provider (SSP) is paid facility that enables the individual or particular organization to outsource their sensitive data to be stored on the server system. It reduces the expense of maintenance of the data. The data owner pays for the some level of security that he wishes and he must make up for amends in case of any bad conduct by the Standalone Service Provider (SSP). On the other hand, the Data owner and authorized users may falsely charges a Standalone Service Provider (SSP) with accuse to get certain amount of compensate or repay. The proposed system has four advantages: A) It allows the owner to outsource sensitive data to SSP, and perform full block level dynamic operations on the data. B) Authorized users can receive the latest version of the outsourced data. C) It creates indirect mutual trust between data owner and SSP. And D) It enforces the access control of the outsourced data can be done by sending a key through email to the registered user.*

Keywords: *Outsourced data storage, Standalone Service Provider (SSP), Unauthorized detection system , Dynamic environment;*

1. INTRODUCTION

The main objective of this system is constructing a secure data storage system that supports multiple functions is challenging when the storage system has no central authority and is

distributed. Since the data owner physically releases sensitive data to a SSP and there are some concerns regarding *integrity*, *confidentiality* and *access control* of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. For verifying data integrity over SSP servers, we have proposed provable data owning technique to validate the entireness of data stored on storage server sites.

Commonly, regular access control techniques assume the presence of the data owner and the storage servers in the same trust domain. This technique, no longer holds when the data is outsourced to a SSP. This technique takes the full charge of the outsourced data handling and stays outside the trust domain of the data owner. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote un trusted SSP. With the help of this solution, the data is encrypted under a certain key, which is shared only with the authorized users. The unauthorized users, including the SSP, are unable to access the data because unauthorized users don't have the decryption key, which is provided by the data owner. This general solution has been broadly incorporated into existing system, which provides data storage security on un trusted storage servers.

This distributed storage system conjointly lets a user forward his information within the storage servers to a different user while not retrieving the information back The distributed storage system not solely supports secure and strong data storage and retrieval, however conjointly lets a user forward his information within the storage servers to a different user while not retrieving the data back. The most technical contribution is that the proxy re-encryption theme supports cryptography operations over encrypted messages yet as forwarding operations over encoded and encrypted messages.

2. RELATED WORK

Existing system is very close to our work in the areas of integrity verification of outsourced data, Cryptographic file systems in distributed networks, and access control of outsourced data. In their protocol, a data owner encrypts the blocks with symmetric data keys, which are encrypted using a master public key. Different variations of both PDP and POR protocols have been presented for data storage system. Based on proxy re-encryption have introduced a secure distributed storage protocol. The data owner keeps a master private key to decrypt the symmetric data keys. Using the master private key and the authorized user's public key, the owner generates proxy re-encryption keys. A semi-trusted server then uses the proxy re encryption keys to translate a cipher text into a form that can be decrypted by a specific granted user, and thus enforces access control for the data. Some other PDP schemes consider the case of dynamic data that are usually more prevailing in practical applications. While the schemes are for a single copy of a data file, PDP schemes have been presented for multiple copies of static data. This is due to encoding of the data file, for example using erasure codes, before outsourcing to remote servers.

Existing research work can be found in the areas of integrity verification of outsourced data, data storage security on untrusted remote servers & access control of outsourced data. The term cloud had already come into commercial use in the early 1990s to refer to large Asynchronous Transfer Mode networks. By 21st century, he term ‘‘cloud computing’’ had appeared, although major focus at this time was on Software as a Service. In 1999, sales-force.com was established by Parker Harris, Marc Benioff. They applied many technologies of consumer web sites like Google and Yahoo! to business applications. They also provided

the concept's like ''On demand'' and ''SaaS'' with their real business and successful customers. Cloud data storage is an important service of cloud computing referred as Infrastructure as a Service .

Amazon's Elastic Compute Cloud and Amazon Simple Storage Service are well known examples of cloud data storage. On the other side along with these benefits' cloud computing faces big challenge i.e. data storage security problem, which is an important aspect of Quality of Service . Once user puts data on the cloud rather than locally, he has no control over it i.e. unauthorized users could modify user's data or destroy it and even cloud server collude attacks. Cloud users are mostly worried about the security and reliability of their data in the cloud. Amazon's is such a good example.

3. PROPOSED SYSTEM

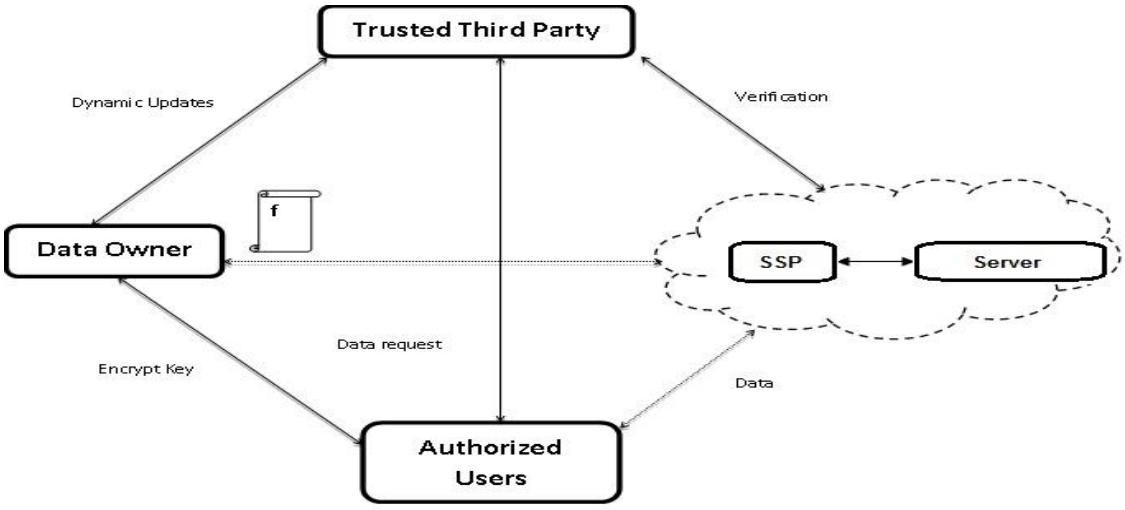

Fig.1: System Architecture

We are trying to provide secure standalone storage system in which we have implemented four modules that are: a) Data Owner Module, b) Standalone Service Provider Module, c) Trusted Third Party Module and d)Authorized Users Module.

The main for module of our system are as follows.

3.1 Data Owner Module:

In this module, we develop the data owner module, where A data owner that can be an organization generating sensitive data to be stored in the cloud and made available for controlled external use. It can be any organization or any individual. First, the data owner has to register with the cloud service provider, to store their data in Cloud Server. After Registering, the data owners gets credential login access using their perspective username and password. The data owner then can upload their files in it. The details of uploaded files are also listed in the separate menu. All the uploaded files are encrypted securely. Only authorized users can only decrypt the file contents uploaded by the data owner. The Data Owner outsource the data to SSP and performs full dynamic operations on the outsourced data at the block level that is insertion, modification, deletion and append etc.

3.2 Standalone Service Provider Module:

In this module we develop the Standalone Service Provider. SSP who manages remote storage servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users. All the files uploaded by the data owner are saved in Storage Server managed by the standalone service providers. We also consider, the SSP is un trusted, and thus the confidentiality and integrity of data in the storage may be at risk. For economic incentives and maintaining a reputation, the SSP may hide data loss, or reclaim storage by discarding data that has not been or is rarely accessed. The Standalone Service Provider plays main role in this system. Also it is working under the Trusted Third Party i.e. TTP.

3.3 Trusted Third Party Module:

In this module, we develop the TTP, a trusted third party (TTP), an entity who is trusted by all other system components, & has capabilities to detect/specify dishonest parties. In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .Also TTP checks the SSP (STANDALONE SERVICE PROVIDER), and find out whether the SSP is authorized one or not. And if the SSP or Authorized user are not authorized then the TTP will not provide the access to them. The TTP is trusted by other three modules that are Data Owner, Authorized User and Standalone Service Provider. It establishes indirect mutual trust between the Standalone Service Provider and the Data Owner, because each party resides in a different trust domain in the system.

3.4 Authorized User Module:

In this module, we develop the authorized user module, where the authorized user is a set of owner's clients who have the right to access the remote data. Also we consider the system model; On the other hand, a data owner and authorized users may collude and falsely accuse the SSP to get a certain amount of reimbursement. They may dishonestly claim that data integrity over storage servers has been violated, or the SSP has returned a stale file that does not match the most recent modifications issued by the owner. It ensures the newness property also, that is the authorized users receive the most recent version of the data outsourced by the data owner to the standalone service provider. It uses the special key provided by the data owner on the secure mail of authorized user. With the help of that key that is decryption key the authorized user can access the data which is he requires. Authorized user is actually the client of the data owner and have to pay only for those resources or data which is he used or accessed.

The relations between various system components are represented by *double-sided* arrows, where solid and dashed arrows represent trust and distrust relations, respectively. For example, the data owner, the authorized users, and the SSP trust the TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the SSP. Thus, the TTP is used to enable *indirect* mutual trust between these three components. There is a direct trust relation between the data owner and the authorized users.

4. CONCLUSIONS

In this conclusion, we have proposed a storage scheme which supports outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data

stored by the SSP, but also updating and scaling this data on the storage 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.

ACKNOWLEDGMENT

We are always thankful to our guide Prof. N. P. Sable for his valuable discussion and constructive suggestions, which greatly contributed to our Paper. We sincerely thank our Head of Department (Comp.) Prof. S. R. Todmal for his reassuring encouragement throughout the preparation of our Paper. We are also grateful to our respected Principal Dr. Sachin Admane sir for his co-operation despite his busy schedule. Last but not the least we thank all the staff members of Computer Department for providing an excellent environment to undergo this Paper.

REFERENCES

[1]. Ayad Barsoum & Anwar Hasan, "Enabling Dynamic Data And Indirect Mutual Trust for Cloud Computing Storage Systems," in proceeding of IEEE Transaction on parallel and distributed system,VOL.24,No.12,DECEMBER 2013.pp.2375

[2]. D. Siva , & R.Mohanavalli Krithika ," Cloud Based Storage Scheme For Indirect Mutual Trust And Outsourcing Dynamic Data," in proceeding of G.J. E.D.T.,Vol.3(2):16-19, March-April, 2014,pp. 2319 – 7293

[3]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, & D. Song, "Provable Data Possession At Untrusted Stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[4]. Q. Wang, C. Wang, J. Li, K. Ren, & W. Lou, "Enabling Public Verifiability And Data Dynamics For Storage Security In Cloud Computing," in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[5]. G. Ateniese, R. D. Pietro, L. V. Mancini, & G. Tsudik, "Scalable And Efficient Provable Data Possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1–10.

[6]. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, & R. Tamassia, "Dynamic Provable Data Possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[7]. Q. Wang, C. Wang, J. Li, K. Ren, & W. Lou, "Enabling Public Verifiability And Data Dynamics For Storage Security In Cloud Computing," in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[8]. A. F. Barsoum & M. A. Hasan, "On Verifying Dynamic Multiple Data Copies Over Cloud Servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011, http://eprint.iacr.org/.

[9]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, & K. Fu, "Plutus: Scalable Secure File Sharing On Untrusted Storage," in Proceedings of the FAST 03: File & Storage Technologies, 2003.