International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enabling Indirect Mutual Trust and Secure Login Mechanism for Cloud Computing Storage Systems

Yasha Gawande[1], Shilpa Gite[2]

[1]Symbiosis International University, SIT, Pune, Maharashtra, India

Abstract: ***In this era, management of huge amount of data is difficult on local machine. Hence many companies are outsourcing their data over remote cloud servers to lessen the storage load. But outsourcing huge amount of sensitive data to cloud servers is risk as cloud servers are untrusted. This work assist user to store data in the form of blocks. The outsourced data should be guaranteed with confidentiality, integrity and access control. In this paper, we propose a scheme which assures these security issues. Also the CSP, data owner and the users share untrust relation, hence trust between these parties is maintained by using a trusted third party (TTP) which has capability to detect and notify fraud party. This paper presents a scheme assuring access control by which data owner can grant or revoke access right to set of users. This cloud storage scheme uses concept of OTP to assert secure login at entry level. Current cloud scheme uses only login id and passwords but using OTP sent over email mitigates the chances of insecure login as OTP can be used only once.***

Keywords: integrity, confidentiality, access control, mutual trust and OTP.

1. Introduction

Cloud computing[1] is a form of computing which enables ubiquitous, on-demand network access, convenient, to a shared pool of configurable computing resources (e.g., networks, applications, services storage, servers) that can be rapidly provisioned with minimal management effort or service provider interaction. In this Information era, several organizations posses huge amount of data which needs to be kept secured. These data includes personal information, health information and financial data. Local maintenance of such huge amount of data will be problematic and cost ineffective. Hence Cloud Service Provider offered Storage as a Service to ease the burden of huge local data storage and to reduce the cost by means of outsourcing data to the cloud. Since the data owner outsources their sensitive data to the cloud, they want their data to be guaranteed with some security concerns like confidentiality, integrity and proper access control. Confidentiality can be guaranteed by encrypting the data before outsourcing it to the remote server. Researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites and for verifying data integrity over cloud servers. Several PDP protocols have been presented to efficiently validate the integrity of data, e.g. POF (Proof of retrievability) [2] was introduced as a stronger technique than PDP in the sense that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers.

Also the outsourced data should not be modified by unauthorized users. This means access control should be guaranteed and restricting access of unauthorized users. Traditional access control techniques assume that the data owner and the storage servers in the same trust domain. However this assumption no longer holds when the data is outsourced to the cloud storage. To enforce access control data is encrypted with certain key and this key is shared only with the authorized users.

In this work, we proposed a technique which addresses some important concerns associated with outsourcing sensitive data to the untrusted remote CSP, such as mutual trust and access control. Mutual trust between the data owner and CSP is enabled in the proposed scheme by using trusted third party (TTP) [3]. A method is presented to resolute dishonest party from any side. Finally, the access control is considered, which gives permission to the data owner to grant or revoke access rights to the outsourced data.

1.1 Key Purposes

The following functionalities are offered by implementation of a cloud-based storage system that has: (i) it allows a data owner to outsource the data to a CSP, and perform operations like upload, delete, and view data (ii) developing an indirect mutual trust between the data owner and the CSP by introducing a trusted third party; and (iii) enabling the access control for the outsourced data.

1.2 Risk Paradigm

While outsourcing data to remote servers, the confidentiality and integrity of data in the cloud may be at risk. So the CSP is untrusted and he may hide data loss for economic incentives and maintaining a reputation or he may delete some data which is rarely accessed for lessening load of management. Furthermore to lessen processing power and to save computational resources of CSP, he may totally ignore or avoid the data-update requests, or may execute a very a few of them. Executing few data update requests leads to violated data on servers which causes CSP to return damaged or stale data for any access request from the authorized users. Various schemes are available which supports the data owner to outsource their sensitive data to the untrusted cloud storage by giving assurance related to the confidentiality, integrity and access control. These schemes identify malicious actions from the CSP side. Sometimes, the CSP may not follow the access rights created by the owner, and

permit unauthorized users to take access which increases risk of misuse of confidential data.
Conversely the CSP also needs to be safeguarded from the dishonest owners, because a data owner or authorized users may collude and falsely claim against the CSP to get a certain amount of compensation. They may fraudulently assert that the data integrity is violated on cloud servers and CSP is not performing data-update requests given by them and returning stale data, thus claiming illegal compensations over CSP. This is risk paradigm and needs to be handled appropriately or this may lead the CSP to go out of business one day [3].

1.3 Security requirements

- *Confidentiality*: outsourced data must be protected from the TTP, CSP, and users that are not granted access.
- *Integrity*: the integrity of outsourced data should be maintained on cloud servers. The data should stay undamaged. the data owner and authorized must detect data corruption over CSP if any.
- *Access control*: only authorized users who are granted to view particular file are allowed to access the outsourced data. *CSP's defense*: the CSP must be safeguarded against false accusations from dishonest owner/users as mentioned in risk paradigm.

2. Related Work

As now a day's many organizations have fear to outsource data on unknown remote servers, most of existing research work can be found in the areas of integrity verification of outsourced data, data storage security on untrusted and unknown remote servers and 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, the term ''cloud computing'' had begin to be seen, although major focus was on Software as a Service (SaaS) at this time. Cloud data storage (Storage as a Service) is an important service of cloud computing referred as Infrastructure as a Service (IaaS). Amazon's Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3) are well known examples of cloud data storage.

Ateniese et al. [4] designed a model based on PDP (Provable Data Possession) protocol which allows a client to verify the server's data possession. In this scheme the client preprocesses the file and generates meta-data, stores it locally, and then outsource the file to the server. The server stores the file and starts respond to challenges issued by the client. Integrity verification is done through batch verification of homomorphic hash functions.

Curtmola et al. [5] designed a model based on MRPDP which uses replication in order to improve data availability and reliability. By storing multiple copies, if some copies are destroyed still the data can be recovered from the remaining copies.
Dodis et al. [6] presented a model based on POR (*Proofs of Retrievability*) in which the client stores a file F on a server and on client side, only a short private verification string is stored locally. Afterwards, the client can run an audit protocol and he verifies the server's data possession, in this technique the client acts as a verifier and the server proves that it possesses the data.

Kallahalla et al. [7] presented a cryptographic based file system called Plutus: Scalable secure file sharing on untrusted storage, which enforces access control over outsourced data. Plutus uses technique by which outsourced file is divided into blocks and each block is encrypted with File-block key and each File-block key is encrypted with File- lockbox key. If the data owner wants to share the file with his clients he just distributes the File- lockbox key to them.

Goh et al. [8] presented SiRiUs, which enforces access control over outsourced data. In this scheme each dfile(data file) is attached with a md-file(meta data file). The md-file contains an encrypted key block for each authorized users with some access right, more precisely the md-file contains d-file's access control list. The d-file is encrypted with FEK and FEK is further encrypted under the public key of each authorized user. Green et al. [9] presented improved proxy re encryption scheme, in which a semi trusted proxy computes a function that converts ciphertext for Alice into ciphertext for Bob without knowing the underlying plaintext.

3. Existing System

Existing scheme addresses important issues related to outsourcing the storage of data, namely *dynamic data*, *newness*, *mutual trust*, and *access control* [3]. 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 this scheme.
The local management of huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Since the data owner physically releases sensitive data to a remote CSP, and CSP and data storage is untrusted, there are some concerns regarding access control, newness, integrity, and confidentiality of the data [10].

To maintain trust and to reduce the computational task in the owner and CSP side, the trusted thread party (TTP) is introduced to reduce generation of block tags and signature. Now validation of outsourced dynamic data and newness property are addressed in existing schema, this is based on combined hash value and a small data structure called *block status table* (BST), as this scheme divides the data into blocks. . Block status table (BST) is a small dynamic data structure used to reconstruct and access the file blocks outsourced to the CSP [3] [10]. The BST contains serial no, block no and key version in which key version helps to guarantees newness property. The TTP established mutual trust among CSP, owner and users. To enforce access control of outsourced data, this schema use cryptographic techniques

like bENC, Key rotation and Lazy revocation. The confidentiality feature can be guaranteed by the owner by encrypting the data file before outsourcing to remote servers. This scheme presents feasible solution guaranteeing newness, integrity, confidentiality and enables the owner to enforce access control of the data stored on a remote untrusted CSP by using a trusted third party [3].

Through this solution, the data is encrypted under a key, which is shared only with the authorized users of data. Now the unauthorized users', including the CSP, does not have the decryption key and thus are unable to access the data. This general solution has been widely incorporated into existing schemes which aim at providing data storage security on untrusted remote servers. On the other hand, the CSP needs to be safeguarded from a dishonest owner, who can claim fraudulent compensations by asserting false charge of data corruption over cloud servers. This scheme addresses important issues related to outsourcing the storage of data, namely dynamic data, mutual trust, newness, and access control. The remotely stored data can be updated and scaled by authorized users, and owner. After updating, authorized users receive the latest version of the data that is technique of key version is used to detect whether the received data is stale or not. Mutual trust between the CSP and the data owner is important issue. For maintaining trust, a mechanism called cheating detection procedure is introduced to determine the dishonest party. Last but not least, the access control is considered, which allows only the authorised users to view data. The owner can grant or revoke access rights to the outsourced data.

4. Proposed System

In this paper, we propose a system that addresses important issues related to outsourcing of storage of data like mutual trust, confidentiality, integrity, and access control. The issue of Mutual trust between the data owner and the CSP is addressed in the proposed system by introducing a concept of trusted third party which is independent entity. Also a mechanism is introduced to determine the dishonest party, i.e., misbehaviour from any side is detected and the responsible party is identified and mail about tampering of data is sent to the owner of data. Last, the access control is considered, which allows only authorised users to view, and download outsourced data. The owner can give permission and he can grant or revoke access rights to the outsourced data to set of users. Proposed scheme uses concept of OTP to enforce access control and a next high security level entry mechanism. OTP is one time password using it for remote cloud server's takes cloud computing to a next security level. As name implies one time password is only valid for one login. The benefit of OTPs is that it offers much higher security than static passwords. OTP is provided to users by means of email id with which they register themselves. OTP is immune against password sniffing attacks, if attackers use software to collect your data traffic, video records you when you type on your keyboard, or use social engineering, it doesn't matter since the password that the attacker gets hold on will not be valid to use [11] [12].

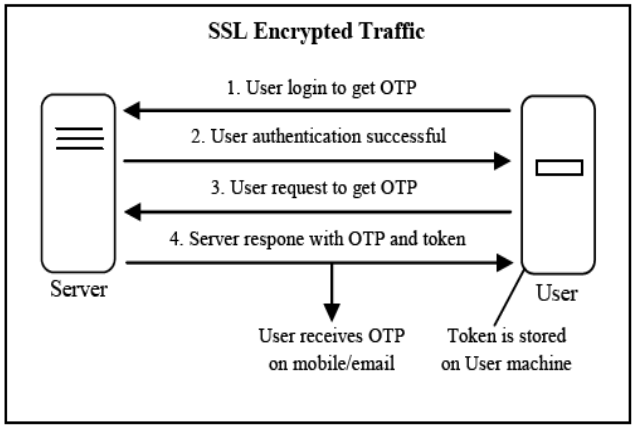

Figure 1: Login by using OTP [12]

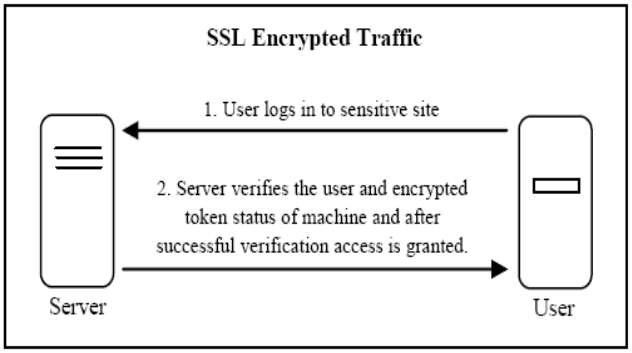

Figure 2: Authenticate user and machine token [12]

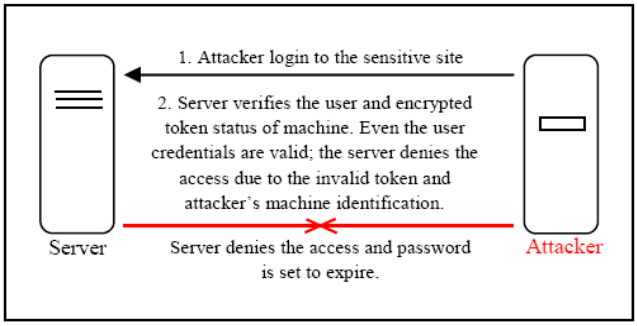

Figure 3: Attackers tries to Access the Sensitive Site [12]

4.1 System Components and Relations

The proposed scheme consists of cloud computing storage model shown in fig. 4 .it consists of four main components. Namely, a data owner that can be anyone who is outsourcing the data to cloud and made available to set of users; a CSP who provides cloud service and manages cloud servers [10]. CSP provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users; authorized users which is a set of owner's clients who have the right to access the remote data; and a trusted third party (TTP) which is an independent entity who is trusted by all other system components that is CSP, Owner and users, and has capabilities to detect and notify dishonest parties [3].

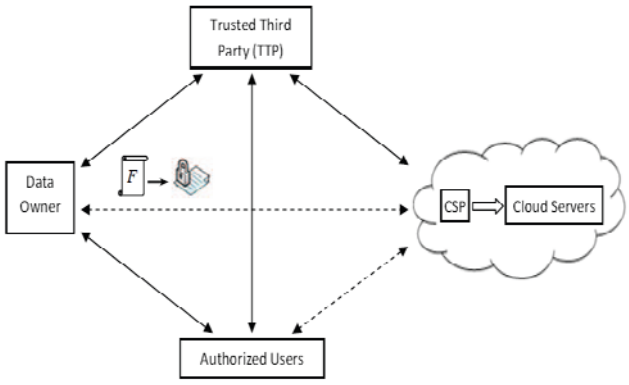

Figure 4: Cloud computing data storage system model [3]

In Fig. 4, the double sided arrows shows the relations between different system components, where solid arrows notify trust relation and dashed arrows represents distrust relations, respectively. For example, the data owner, the authorized users, and the CSP have solid arrow with TTP, this means they trust TTP. On the other hand, the data owner and the authorized users have mutual distrust relations with the CSP shown by dashed arrows. Thus, the TTP establishes *indirect* mutual trust between the three components that is CSP, owner, and authorized users. There is a direct trust relation between the data owner and the authorized users [3].

4.2 Outsourcing, updating, and accessing

The file uploaded by data owner is divided into several blocks. For confidentiality, the file gets encrypted by using RC5 and then it is stored in the form of blocks on cloud server. We are storing file in the form of blocks and these blocks are not saved sequentially into the database, so in case of any tampering onto data, we can save maximum portion of file from getting damaged. After successful data outsourcing to cloud, the owner and the authorized users can interact with the CSP to perform operations on the file like view and download. The owner has rights to make his outsourced file visible to set of users. That means owner can grant or revoke access rights of user on a particular file, in other words owner can share the file with set of users and these users are given permission to download the outsourced file. When owner uploads file to cloud server, file is stored in encrypted format and data hashes are calculated. These hashes are maintained on CSP side, and one copy of these data hashes is stored at TTP which are periodically cross verified. The TTP is an independent entity, and thus has no reason to collude with any party. If these hashes do not match with each other, TTP send mail to owner about data tampering. The TTP and the CSP are always online, while the owner is intermediately online. The authorized users are able to access the data file from the CSP even when the owner is offline.

4.3 Advantages of proposed system

- It allows the owner to outsource sensitive data to a CSP.
- It allows the authorized users (i.e., those who have the right to access the owner's file) to download and view the outsourced data.
- It enables authorized users to share particular file with other list of users
- It enables indirect mutual trust between the owner and the CSP.
- It allows the owner to grant or revoke access to the outsourced data.
-

4.4 Modules Description

4.4.1 Data Owner Module

In this module, we develop the data owner module. A data owner can be anyone generating sensitive data to be stored on the cloud and made available for authorised users. Firstly, the data owner needs to register with the cloud service provider by filling certain details including login id, password, and email id. After Registering, the data owners gets a system generated security token which he has to store on his local machine. Now while login he needs to give credentials like login id, password and security token. After entering correct credentials, owner gets OTP (one time password) on his mail id, on providing this OTP the login process will complete. This OTP can be used only one time so using OTP will enforce access control on users of cloud. Now after login user can perform operations like upload data, view, and share data with list of users.

4.4.2 Cloud Service Provider Module

In this module we develop the Cloud Service Provider. CSP is entity who manages remote cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users. We consider, the CSP is untrusted, and thus the confidentiality and integrity of data in the cloud should be guaranteed. Thus the data is stored on CSP in encrypted format. And as discussed in section risk paradigm, for economic incentives and maintaining a reputation, the CSP may hide data loss, or delete some data which is rarely accessed owner and users.

4.4.3 Authorized Users Module

In this module, we develop the authorized user module. The authorized user is a set of owner's clients who have given permission to access the remote data stored by the owner. As discussed in section risk paradigm, a data owner and authorized users may fraudulently charge CSP to get a certain amount of reimbursement by dishonestly claiming violation of data integrity over cloud servers. Also they may falsely accuse the CSP for returning a stale file. Authorised users also need to register themselves and they will get same system generated security token as in owner module. After providing the credentials they will also get OTP on their registered email id, and after filling correct OTP, user will get access to cloud remote server. Any file shared or granted by owner is accessible to user in shared data tab.

4.4.4 Trusted Third Party (TTP) Module

In this module, we develop the TTP, a trusted third party (TTP), an independent entity who is trusted by all other system components. It has capabilities to detect/specify dishonest parties. For detecting dishonest party it uses mechanism of comparing hashes of data. If hashes of CSP do not match with the one on TTP side, email is generated and

sent to owner. In this module TTP monitors the data at owner side and CSP side periodically.

5. Result Analysis and Evolution

We evaluate the performance of the proposed scheme by analyzing storage and computation overhead. We have tested the proposed scheme on system with windows 7, 4GB RAM, Intel core i5 processor and java. The result is evaluated in the form of graph showing OTPLogin time on x-axis in milliseconds against load on y-axis for 10 users. OTPLogin time is very less; this shows that addition of OTP does not increase computation overhead. The data file we have used for our experimental testing are of size 1MB to 100MB with block size of 100KB. Evaluating Storage overhead, both entries in BST at the owner side and CSP side are checked which are only of 8bytes size.

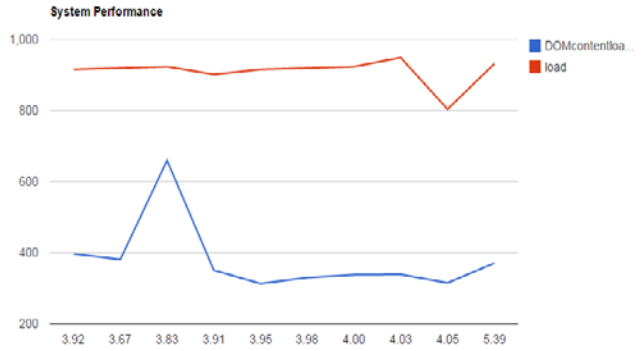

Figure 5: System performance

6. Conclusion

In this paper, we have presented a cloud-based storage scheme which uses concept of OTP to ensure access control where the owner is capable of uploading, downloading and sharing data with set of users. Also owner of file can give access rights by granting or revoking the access of particular file with set of users. This provides flexibility to cloud users to view data to limited clients. Moreover, in case of dispute regarding data integrity/newness, a TTP is able to determine the dishonest party. Also we are storing file in the form of blocks, which saves whole file from getting tampered. The proposed scheme provides 3 level secure accesses to remote cloud: 1.user id and password 2.OTP by mail, 3. Cryptography by RC5 .The experimental results show that the proposed scheme is a robust model in terms of security and access control.

References

[1] NIST SP 800-145, “A NIST definition of cloud computing”,http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
[2] Y. Dodis, S. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC ’09: Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 109–127.
[3] A. F. Barsoum and M. A. Hasan, ”Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems” IEEE Transactions on Parallel and Distributed Systems, 2012.
[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in CCS ’07: Proceedings of the 14th ACM Conference on Computer and Communications Security, New York, NY, USA, 2007, pp. 598–609.
[5] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, “MR-PDP: multiple replica provable data possession,” in 28th IEEE ICDCS, 2008, pp. 411–420.
[6] Y. Dodis, S. Vadhan, and D. Wichs, “Proofs of retrievability via hardness amplification,” in TCC ’09: Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 109–127.
[7] 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 Conference on File and Storage Technologies, USENIX, 2003.
[8] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing remote untrusted storage,” in Proceedings of the Network and Distributed System Security Symposium, NDSS. The Internet Society, 2003.
[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, “Improved proxy re-encryption schemes with applications to secure distributed storage,” in Proceedings of the Network and Distributed System Security Symposium, NDSS. The Internet Society, 2005.
[10] P. Sathyabama Gayathri, J. Angela Jennifa Sujana, T.Revathi, “Enhancing Security of Dynamic Data for Storage Services In Cloud Computing” in International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014.
[11] Indrajit Das, Ria Das, “Mobile Security (OTP) by Cloud Computing”, International Journal of Innovations in Engineering and Technology,vol. 2, issue 4, augest 2013.
[12] Ahmad Alamgir Khan, “Preventing Phishing Attacks using One Time Password and User Machine Identification”, International Journal of Computer Applications (0975 – 8887) Volume 68– No.3, April 2013.

Author Profile

Yasha Gawande received the B.E. degree in Computer Science Engineering from Kavikulguru Institute of Technology, Ramtek, Nagpur, Maharashtra in 2012. Currently pursuing M.Tech in computer Science from Symbiosis Institute of Technology and area of interest is parallel and distributed computing.