ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Provable Dynamic Multi Data Copy Possession in Cloud Storage

Sneha Josmi Sam[1], Vinodu George[2]

PG Scholar, Department of Computer Science, LBS College of Engineering, Kasaragod[1]

Professor, Department of Computer Science, LBS ITW, Thiruvanathapuram[2]

Abstract: Many individuals and organizations are seeking to reduce the maintenance cost and the burden of large local data storage. So outsourcing of data to remote Cloud Service Providers (CSPs) increased drastically. Customers can rent the CSPs storage infrastructure to store and retrieve unlimited amount of data by paying money. Higher level of scalability, availability, and durability are achieved by replicating data on multiple servers across multiple data centers. More the copies are requested to store in the cloud more fees have to be paid. Since more fees are paid customers needs to ensure whether requested copies are stored with most recent modification. In existing methods a Provable Multi Copy Dynamic Data Possession (PMDDP) scheme is used. It gives evidence to the customers that the CSP is not cheating them by storing fewer copies. It supports outsourcing of dynamic data. It supports modification, insertion and deletion of data stored in the cloud. Even though possession of multiple copies of data can be proved, user cannot ensure whether the data is stored in different servers or locations. In this proposed system, user can ensure that multiple data copies are stored in different locations.

Keywords: Cloud computing, Cloud Service Provider, Data owner, dynamic environment.

I. INTRODUCTION

Cloud Computing (CC) is an emerging computing paradigm that can offer multiple advancements. Outsourcing data to a remote cloud service provider (CSP) allows organizations to store more data on the CSP than on private computer systems. Such outsourcing of data to CSP helps organizations from computing issues and to concentrate more on innovations. All the authorized users can retrieve data from different locations in the world from CSP. The data owners lose the direct control over their sensitive data once the data has been outsourced to a remote CSP which need not be trustworthy. This lack of control over their sensitive data raises new omnious and challenging tasks related to data confidentiality and integrity maintenance in cloud computing. The confidentiality issue can be solved by encrypting the data before outsourcing to cloud storage. As such, it is a high priority demand of customers to have strong evidence that the cloud servers still possess their data and it is not being tampered with or partly deleted over time. Accordingly, many researchers have focused on the problem of Provable Data Possession (PDP) and proposed different techniques to review the data over remote servers. PDP is a technique to approve data integrity over remote servers.

In a typical PDP model, some metadata/information are generated by the data for a data file to be used later for verification purposes through a challenge-response protocol with the remote/cloud server. The owner sends the file to be stored on a remote server which may be untrusted, and deletes the local copy of the file. As a proof that the server still possesses the data file in its original form, it needs to correctly compute a response to a challenge vector sent from a verifier. Verifier can be the original data owner or a trusted entity that shares some information with the owner. Researchers have proposed different variations of PDP schemes under different cryptographic assumptions. One of the core design principles of outsourcing data is to provide dynamic behaviour of data for various applications as in [7]-[10]. This means that the remotely stored data can be not only accessed by the authorized users, but also updated and scaled by the data owner. Some PDP schemes are focused only on static or warehoused data as in [4]-[6], where the outsourced data is kept unchanged over remote servers. Most of the PDP schemes dealing with dynamic data is for single copy. When verifying multiple data copies, the overall system integrity check fails if there are one or more corrupted copies.

A. Existing System

Some PDP schemes are focussed on static or warehoused data. Outsourced data is kept unchanged over remote sources. Since the data cannot be changed data might become outdated as in [4]-[6]

Some PDP schemes deal with dynamic data. That is, the data can be modified with users' requirement. But they deal with single copy of data as in [7]-[10].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

The Existing System provides an adequate guarantee that the CSP store all the copies of data that are agreed upon in the contract as in [1]-[3]. Data owner creates the copies of the file and divide each file into blocks. These files are encrypted and is outsourced to the CSP. The scheme supports outsourcing of dynamic data. CSP maintains the files that are outsourced to it. It provides block level operations such as modification, insertion, deletion. Data owner sends a challenge to the CSP to check whether the agreed copies are stored in the CSP. As soon as the challenge is received it computes a proof and sends it to data owner. Data owner or the verifier verifies the proof and confirms that agreed number of copies are stored in the CSP. The authorized users who are legitimate to access the owner's file can access the copies seamlessly from the CSP. It provides authentication, integrity and confidentiality. It supports public verifiability even though he neither possesses nor retrieves the file from the cloud server.

B. Proposed System

Existing system provides adequate guarantee that the CSP store all the copies of data that are agreed upon in contract. But it does not provide any proof whether the copies of the data are stored in different locations over different servers.
In the proposed scheme data owners divide the file into blocks then it generate keys needed for the sessions. Then the blocks are encrypted and it is outsourced to the CSP. CSP receives the file and generate the copies of the as per in the contract. Then it send the file copies to respected locations and CSP creates location tags with location details. These location tags are shared with the data owner. Data owner send a challenge to the CSP for getting the proof. This can be done by an interactive zero knowledge protocol. Interactive zero knowledge protocol is a method in which one party can covey to the other party that the given statement is true. Non interactive protocol different class of Zero-Knowledge proof systems, where no interaction is required: The Prover simply sends one message to the Verifier, and the Verifier either accepts or rejects. Interactive zero knowledge protocol is used at the time of verification. From each location a proof is generated and is send to the data owner to verify. Verifier verifies the proof. CSP maintains insertion, deletion, modification of the blocks in the CSP. Authorised users can access the file by getting a shared key from the Data owner.

II. SYSTEM DESIGN

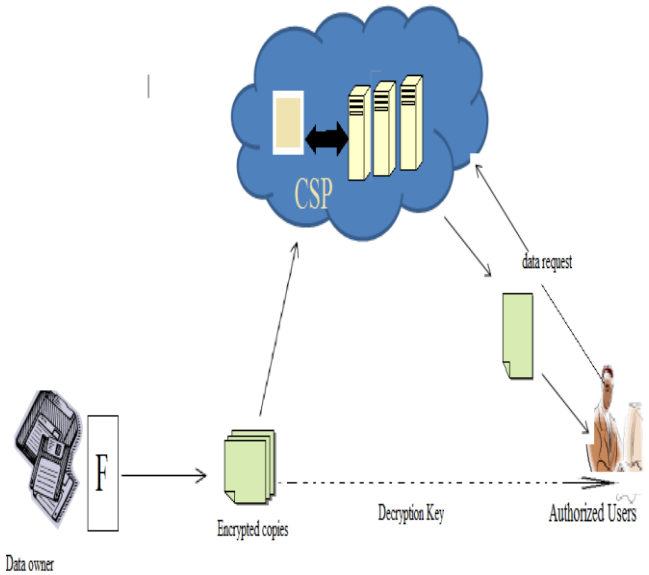

Fig 1: cloud computing data storage model

The cloud computing data storage model considered in this work consists of three main components as illustrated in Fig. 1: (i) A data owner that can be an organization outsourcing data to the cloud server (ii) a CSP who manages cloud servers (CSs) and it provides paid storage space on its infrastructure to store owner's files and (iii) authorized users — a set of owner's clients who have the right to access the remote data seamlessly. The storage model used in this work can be adopted by many of the practical applications. For example, e-Bank applications can be picturized by this model where the client's database that contains large and sensitive information can be stored on the cloud servers. In these types of applications, the e-bank can be considered as the data owner, and the employees as the authorized users who have the right to access the clients' banking history. Many other practical applications like financial, scientific, and educational applications can be viewed in similar settings.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

A. Protocol Design

i) Data Owner:-

- Data owner generates keys that are required for sessions.
- It divides the files into blocks.
- These blocks are encrypted.
- These blocks are outsourced to the CSP.
- It receives location tags from the CSP and maintains the location details in it.
- It challenges the CSP to provide proof. It sends challenge to the CSP to verify whether the agreed number of copies are stored in the CSP.
- Proof is received by the data owner from different locations that are specified in the tags.
- After receiving the proof, proof is verified. If proof is correct then the exact copies of the files are maintained in the CSP. Then the data owner confirms reliability with the CSP.
- When the authorized users request to grant permission to access the file, data owner will share a key with the user and user will access the file with it.

ii) Cloud Service Provider:-

- CSP receives the file blocks outsourced to it.
- CSP creates multiple copies that agreed with the data owner.
- It sends the file copies to the location.
- After sending the file to location, tags are created with the details of the location.
- These created location tags are send to data owner.
- CSP receives a challenge from the data owner.
- When challenge is received, it is passed to the locations where the copies are stored.
- Each location computes a proof and these proofs are passed to the data owner with interactive zero knowledge protocol.
- Operations like insertion, deletion, modification, append are performed in the CSP on file blocks according to data owners' request. Insertion insert a block anywhere in the file. Deletion deletes the block completely. Modification modifies the block content. Append operation adds a new block at the end of the blocks.
- After the operation change must be updated to all the copies present in the CSP.
- Request for accessing the file is received from the authorized users.
- After checking the authenticity encrypted blocks are send to the authorized users.

iii) Authorised Users:-

- Authorized users request the data owner to grant permission to access the file from the CSP.
- It will receive a key from the data owner.
- After receiving the key, it will request for the file to the CSP.
- User will receive the encrypted blocks of the file in an unordered manner.
- Blocks are decrypted using the Shared secret key. These blocks are rearranged to get a complete file. Every file can be decrypted with the same key. Users can seamlessly access the file from the CSP.

III. COMPARISON

Existing system assures the data owner that exact copies of the file are stored in the cloud service provider. But it does not give any evidence whether the file copies are stored in different location.
The proposed system provides a proof to the data owner that the data copies are stored in different location. So the system is more reliable than the existing system. In this, CSP creates multiple copies that are agreed upon the contract. So data owner need to send only one copy, it need not send same files in multiple copies. So the traffic that occur while outsourcing the file to the CSP can be reduced. In this, each location computes a proof when the data owner challenges. So the computation will be more. Even though the computation is more, CSP can earn more trust from the data owner.

IV. CONCLUSION

Outsourcing data to remote servers has become for many organizations to diminish the burden of local data storage and maintenance. In this work the problem of creating multiple copies of dynamic data in cloud storage and verifying those copies stored on untrusted cloud servers is discussed.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

IJARCCE

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

In this work a new PDP scheme is introduced, which supports outsourcing of multi-copy data. Data owner is capable of archiving and accessing the data copies stored by the CSP. Data owner can also confirm that the data copies are stored in the correct numbers and in different location.

Authorized users can interact with CSP, where the authorized users can seamlessly access a data copy received from the CSP using a single secret key shared with the data owner. Proposed scheme supports public verifiability, enables auditing, and allows possession free verification where the verifier has the ability to verify the data integrity even though he neither possess nor retrieved the file block from the server.

REFERENCES

[1]. F. Barsoum and M. A. Hasan.(2015) "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems" IEEE transactions

[2] A. F. Barsoum and M. A. Hasan. (2010). "Provable possession and replication of data over cloud servers," Centre Appl. Cryptograph. Res., Univ. Waterloo, Waterloo, ON, USA, Tech. Rep. 2010/32. [Online]. Available:

[3] A. F. Barsoum and M. A. Hasan. (2011). "On verifying dynamic multiple data copies over cloud servers," IACR Cryptology ePrint Archive, Tech. Rep. 2011/447. [Online]. Available: http://eprint.iacr.org/

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw. (SecureComm), New York, NY, USA, 2008, Art. ID 9

[5] C. Wang, Q. Wang, K. Ren, and W. Lou. (2009). "Ensuring data storage security in cloud computing," IACR Cryptology ePrint Archive, Tech. Rep. 2009/081. [Online]. Available: http://eprint.iacr.org/

[6] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2009, pp. 213–222.

[7] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[8] K. Zeng, "Publicly verifiable remote data integrity," in Proc. 10th Int. Conf. Inf. Commun. Secur. (ICICS), 2008, pp. 419–434.

[9] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[10] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," IACR (International Association for Cryptologic Research) ePrint Archive, Tech. Rep. 2006/150, 2006.