GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)

www.gifre.org

CLOUD BASED STORAGE SCHEME FOR INDIRECT MUTUAL TRUST AND OUTSOURCING DYNAMIC DATA

D.Siva [1], & R.Mohanavalli Krithika [2]

[1]M.Tech (CSE) Student, Department of CSE, S.R.M. University,Ramapuram Campus, Chennai,India.
[2]Assistant Professor, Department of CSE, S.R.M. University, Ramapuram Campus, Chennai,India.

Abstract

Presently, the huge amount of perceptive data produced by numerous organizations is outpacing their storage ability. A data owner pays for a desired level of security and must get some compensation in case of any misbehavior committed by the CSP. Storage-as-a-Service (SaaS) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their data to be stored on remote servers. Thus, SaaS reduces the maintenance cost and moderate the burden of large local data storage at the organization's end. In this paper, we propose a cloud-based storage method that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four significant features: First one, it allows the owner to outsource perceptive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append. Second one, it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the recent version of the data outsourced. Next one, it enables indirect mutual trust between the owner and the CSP. Last one, it allows the owner to grant or revoke access to the data outsourced. We discuss the security issues of the proposed scheme. Besides, we justify its performance through hypothetical analysis, prototype implementation and evaluation of storage, communication, and computation overheads towards the cloud computing environment.

Keywords: *Storage-as-a-Service (SaaS), Cloud Service Providers (CSP), Mutual Trust, Access Control, Outsourcing Data Storage.*

I. Introduction

Cloud computing has conventional significant consideration from both academic intuitions' and IT industry due to a number of essential advantages including: cost effectiveness, low management overhead, immediate access to a wide range of applications, flexibility to scale up and down information technology (IT) capacity, and mobility where customers can access information wherever they are, rather than having to remain at their desks. Cloud computing is a distributed computational model over a large pool of shared-virtualized computing resources (e.g., storage, processing power, memory, applications, service and network bandwidth).Cloud Service Provider(CSPs) offer different types of services as 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, different organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data.

SaaS offered by CSPs is an emerging solution to mitigate the burden of large local data storage and reduce the maintenance cost via the concept of outsourcing data storage. Through outsourcing data storage scenario, data owners delegate the storage and management of their data to a CSP in exchange for pre-specified fees metered in GB/month. Such outsourcing of data storage enables owners to store more data on remote servers than on private computer systems. Moreover, the CSP often provides better disaster recovery by replicating the data on multiple servers across multiple data centers achieving a higher level of availability. Thus, many authorized users are allowed to access the remotely stored data from different geographic locations making it more convenient for them. Since the owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. In some practical applications, data confidentiality is not only a privacy concern, but also a juristic issue. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. . For verifying data integrity over cloud servers, developer have proposed provable data possession technique to validate the intactness of data stored on remote sites. A number of PDP protocols have been presented to efficiently validate the integrity of data. Proof of irretrievability 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. 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 data owner to grant or revoke access rights to the outsourced data

The main contributions cloud based storage can be discussed in different aspects;

(1).The design and implementation of a cloud-based storage scheme that has the following features:

(a). It allows a data owner to outsource the data to a remote CSP, and perform full dynamic operations at the block-level, i.e., it supports operations such as block modification, insertion, deletion, and append.

(b). It ensures the newness property, i.e., the authorized users receive the most recent version of the data.

(c). It establishes indirect mutual trust between the data owner and the CSP since each party resides in a different trust domain.

(d). It enforces the access control for the outsourced data.

(2).We discusses the security features of the proposed scheme. Besides, we justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overhead.

II. Related Work

Existing research close to our work can be found in the areas of integrity verification of outsourced data, Cryptographic file systems in distributed networks, and access control of outsourced data. Different variations of both PDP and POR protocols have been presented for static or data warehouse. Based on proxy re-encryption have introduced a secure distributed storage protocol. In their protocol, a data owner encrypts the blocks with symmetric data keys, which are encrypted using a master public key. 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. Reference addresses a PDP construction for multiple copies of dynamic data. Proof of Retrievability (POR) is a complementary approach to PDP, and is stronger 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. This is due to encoding of the data file, for example using erasure codes, before outsourcing to remote servers.

III. Literature Survey

We have to analysis the cloud based storage Outline Survey: Cloud computing provide much more effective computing by centralized memory processing, storage and bandwidth. The problem in cloud computing is that they are facing a potentially formidable risk for missing or corrupted data. Third party auditor should be able to efficiently audit the cloud data storage without demanding the local copy of data. DES algorithm can use for encryption in CSP. In this paper, we propose to implement the mobile devices that can be interfaces in between the Cloud Service Provider and Third party Agent to avoid the delay in sending the modification done in the data storage to the cloud and also client's owner. Also we implement a user authentication protocol named Pass which leverages a user's cell phone and short message service (SMS) to prevent password stealing and password reuse attacks in cloud computing we demonstrate to decrease the delay through mobile device. Our simulation results for the cost, computational and communication overhead can perform more effective in cloud computing. Secure distributed data storage can shift the burden of maintaining a large number of files from the owner to proxy servers. Proxy servers can convert encrypted files for the owner to encrypted files for the receiver without the necessity of knowing the content of the original files. In practice, the original files will be removed by the owner for the sake of space efficiency. Hence, the issues on confidentiality and integrity of the outsourced data must be addressed carefully. However, moving the infrastructure and sensitive data from trusted domain of the data owner to public cloud will pose severe security and privacy risks. It enables senders to encrypt messages under a set of attributes and private keys are associated with access structures that specify which cipher texts the key holder will be allowed to decrypt.

IV. Proposed System Model

The cloud computing storage model considered in this work consists of four main components as illustrated in Fig. 1: (i) a data owner that can be an organization generating sensitive data to be stored in the cloud and made available for controlled external use; (ii) a CSP who manages cloud servers and provides paid storage space on its infrastructure to store the owner's files and make them available for authorized users; (iii) authorized users – a set of owner's clients who have the right to access the remote data; and (iv) a trusted third party (TTP), an entity who is trusted by all other system components, and has expertise and capabilities to detect and specify dishonest parties and who is trusted by all other system components.

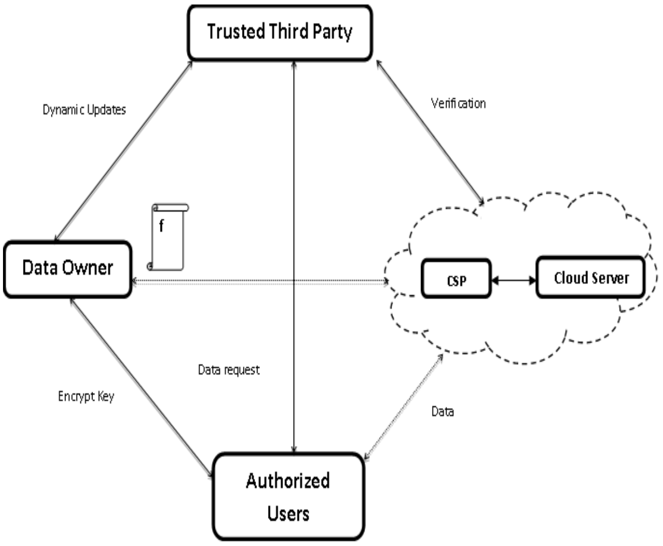

Fig. 1: Cloud computing data storage system model

Cloud computing data storage system model have different mechanism used; First one, Data Client is the **c**lient uses the services provided by the owner. Client access the data provided by the owner through the Cloud server. But cloud server is an invisible entity to the client. The client should be an authenticated user to the data owner. Second one, Data Owner is the owner use Cloud server to store the data. The owner provides data to the end users through the Cloud Server. The owner provides on demand services to the user. Key is generated by the Owner. The data is encrypted using the private key of the owner and public key is transferred along with the data. Authorized users can only decode it. Third one, CSP is **c**loud server act as a platform to store the owner's data to be accessed by the Client. Many owners can use the same Cloud server to provide services to their set of users. In this module CSP has to get the key first. Then only he can store the file in his cloud server.TTP can only check the CSP whether the CSP is authorized or not. If it is not authorized, TTP won't allow the file to store in cloud server. Finally, 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 CSP and find out whether the CSP is authorized one or not.

V. System Preliminaries

Lazy Revocation**:** The proposed scheme in this work allows the data owner to revoke the right of some users for accessing the outsourced data. In lazy revocation, it is acceptable for revoked users to read (decrypt) unmodified data blocks. Key Rotation**:** Key rotation is a technique in which a sequence of keys can be generated from an initial key and a master secret key. The sequence of keys has two main properties: (i) only the owner of the master secret key is able to generate the next key in the sequence from the current key, and (ii) any authorized user knowing a key in the sequence is able to generate all previous versions of that key. In other words, given the i-th key Ki in the sequence, it is computationally infeasible to compute keys Ki for l > i without having the master secret key, but it is easy to compute keys Kj for j < i.Whenever a user's access is revoked, the data owner generates a new key in the sequence (rotating forward). Let ctr indicate the index/version number of the current key in the keys sequence. The owner generates the next key by exponentiation Kctr with the master secret key d: Kctr+1 = Kd ctr mod N. Authorized users can recursively generate older versions of the current key by exponentiating with the public key component e: Kctr-1 = Kectr mod N (rotating backward). The RSA encryption is used as a pseudorandom number generator; it is unlikely that repeated encryption results in cycling, for otherwise, it can be used to factor the RSA modulus N.Broadcast Encryption**:**Broadcast encryption (bENC) allows a broadcaster to encrypt a message for an arbitrary subset of a group of users. The users in the subset are only allowed to decrypt the message. However, even if all users outside the subset collude they cannot access the encrypted message. Such systems have the collusion resistance property, and are used in many practical applications including TV subscription services and DVD content protection.Block Status Table**:** The block status table (BST) is a small dynamic data structure used to reconstruct and access file blocks outsourced to the CSP. The BST consists of three columns: serial number (SN), block number (BN), and key version (KV). SN is an indexing to the file blocks. It indicates the physical position of each block in the data file. BN is a counter used to make a logical numbering/indexing to the file blocks.

VI. Dynamic Operations On The Outsourced Data

The dynamic operations in the proposed scheme are performed at the block level via a request in the general form {BlockOp, TEntry BlockOp, j,KVj; h(bj), RevFlag,; b*}. Where BlockOp corresponds to block modification (denoted by BM), block insertion (denoted by BI), or block deletion (denoted by BD). TEntry ,Block Op indicates an entry in BST corresponding to the issued dynamic request. The parameter j indicates the block index on which the dynamic operation is to be performed, KVj is the value of the key version at index j of BST before running a modification operation, and h(~bj) is the hash value of the block at index j before modification/deletion. RevFlag is a 1-bit flag (true/false and is initialized to false) to indicate whether a revocation has been performed, and b is the new block value.Modification:.Data modification is one of the most frequently used dynamic operations in the outsourced data. For a file F=fb1;b2;:::;bmg, suppose the owner wants to modify a block bj with a block b0j. It describes to performed by each system component (owner, CSP, and TTP) during block modification. The owner uses the technique of one-sender-multiple-receiver (OSMR) transmission to send the modify request to both the CSP and the TTP. Insertion: In a block insertion operation, the owner wants to insert a new block B after index j in a file F =fb1;b2;:::;bmg, i.e., the newly constructed file F0=fb1;b2;:::;bj;b;:::;bm+1g,where bj+1=b. The block insertion operation changes the logical structure of the file, while block modification does not. Fig. 4 describes the steps performed by each system component (owner, CSP, and TTP) during block insertion. Append:Block append operation means adding a new block at the end of the outsourced data.It can simply be implemented via insert operation after the last block of the data file.

VII. Experimental Evaluation

In this section we experimentally evaluate the computation overhead the proposed scheme brings to a cloud storage system that has been dealing with static data with only confidentiality requirement. The experiments are conducted using NETBEANS on a system with an Intel(R) 2-GHz processor and 3GB RAM running Windows XP. Algorithms (hashing, broadcast encryption, digital signatures, etc.) are implemented using MIRACL library version 5.5.4. For a 128-bit security level, bENC uses an elliptic curve with a 256-bit group order. In the experiments, we utilize SHA-256, 256-bit BLS signature, and Bar-reto-Naehrig (BN) [50] curve defined over prime field GF(p) with p = 256 bits and embedding degree = 12 (the BN curve with these parameters is provided by the MIRACL library). To evaluate the computation overhead on the owner side due to dynamic operations, we perform 100 different block operations from which 50% are executed following revocations (this percent is higher than an average value in practical applications).Scalability (i.e., how the system performs when more users are added) is an important feature of cloud storage systems. The access control of the proposed scheme depends on the square root of the total number of system users. To identify the dishonest party in the system in case of disputes, the TTP verifies two signatures (F and T), computes combined hashes for the data (file and table), and compare the computes hashes with the authentic values (THTTP and FHTTP). Thus, the computation overhead on the TTP side is about 10.77 seconds. Through our experiments, we use only one desktop computer to simulate the TTP and accomplish its work. In practice, the TTP may choose to split the work among a few devices or use a single device with a multi-core processor which is becoming prevalent these days, and thus the computation.

In the worst case, the TTP executes only 4 hashes per dynamic request to reflect the change on the outsourced data. Thus, the maximum computation overhead on the TTP side is about 0.08 milliseconds, i.e., the proposed scheme brings light overhead on the TTP during the normal system operations. The computation overhead on the user side due to data access comes from five aspects divided into two groups. The first group involves signatures verification and hash operations to verify the received data (file and table). The second group involves broadcast decryption, backward key rotations, and hash operations to compute the DEK.

VIII. Conclusion

Outsourcing data to remote servers has become a growing trend for many organizations to alternative the burden of local data storage and maintenance. In this work we have studied different aspects of outsourcing data storage: dynamic data, newness, mutual trust, and access control. Dynamic data is indicating the data can be update that is asynchronously altered as additional updates to the information become accessible. Authors have projected a cloud-based storage idea which supports outsourcing of dynamic data, wherever the owner of data is capable of not only modifying and grading this data on the remote servers, but also accessing and archiving the data stored by the CSP. 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. We have examined the expenses added by our method when included into a cloud storage model for fixed data with security and privacy requirement.

References

[1]C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in INFOCOM, 2010.

[2]W. Wang, Z. Li, R. Owens, and B.Bhargava, “Secure and efficient access to outsourced data,” in Proceedings of the 2009 ACM workshop on Cloud computing security, ser. CCSW ’09. ACM, 2009..

[3]C. Erway, A. Kupu, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in CCS’09: Proceedings of the 16th ACM Conference on Computer and Communications Security, New York, NY, USA, 2009.

[4]G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in SecureComm ’08: Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, New York, NY, USA, 2008.

[5]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..

[6]M. J. Atallah, K. B. Frikken, and M. Blanton, “Dynamic and efficient key management for access hierarchies,” in Proceedings of the 12th ACM Conference on Computer and Communications Security, ser. CCS ’05. ACM, 2005,

[7]K. D. Bowers, A. Juels, and A. Oprea, “HAIL: a high-availability and integrity layer for cloud storage,” inCCS ’09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009.

[8] A. F. Barsoum and M. A. Hasan, “On verifying dynamic multiple data copies over cloud servers,” Cryptology ePrint Archive,Report 2011.