International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 1, January- 2013

A Survey On Different Encryption Schemes And Security Challenges In Cloud Storage System

Helen Sara George
PG Scholar
Department of Computer Science & Engg
Karunya University

Mrs.Jeno Lovesum
Assistant Proffessor(SG)
Department of Computer Science & Engg
Karunya University

Abstract

Security of storing data in cloud is challenging. Availability and retrievability of the data to the authenticated ones are done with different levels of security pass. When compared to all the previous methods and security measures, the newly proposed threshold proxy re-encryption scheme and erasure codes over exponents improved security in this paper. The threshold proxy re-encryption scheme supports encoding and data forwarding, and partial decryption operations over encoded data in a distributed way. Key servers act as access nodes for providing a front-end layer such as a traditional file system interface. Each storage server independently performs encoding and re-encryption and each key server independently performs partial decryption .All these new enhanced methods can provide a secure data forwarding..

1. Introduction

Cloud computing and virtualization in cloud computing is an emerging technology .The concept of Cloud computing is somewhat similar to large scale distributed system. It is impossible to clearly specify the beginning of cloud computing technology. When we delve into cloud computing technology, it shows that the computing methodologies in cloud started from mainframe computers. Storing data in distributed databases creates great concern to the integrity and confidentiality of data stored. This paper is based on the survey of security challenges in cloud storage system from different perspectives.

2. Data Routing

In Oceanstore:An architecture for global-scale persistent storage, data is secured through replication methods and cryptographic methods. Performance can be improved by caching, data in different storage servers at, any time. Additionally, monitoring of usage patterns allows adaptation to regional outages and denial of service attacks; monitoring also enhances the performance through proactive movement of data[1]. The main two concepts involved in this is untrusted infrastructure and nomadic data that is servers are like “pools” in which data is allowed to flow freely as shown in Fig 1.

Objects in data store can reside any of the oceanstore servers. This provided versatility in techniques like cashing, replication and migration .

In PAST:A large-scale, persistent peer-to-peer distributed storage utility .

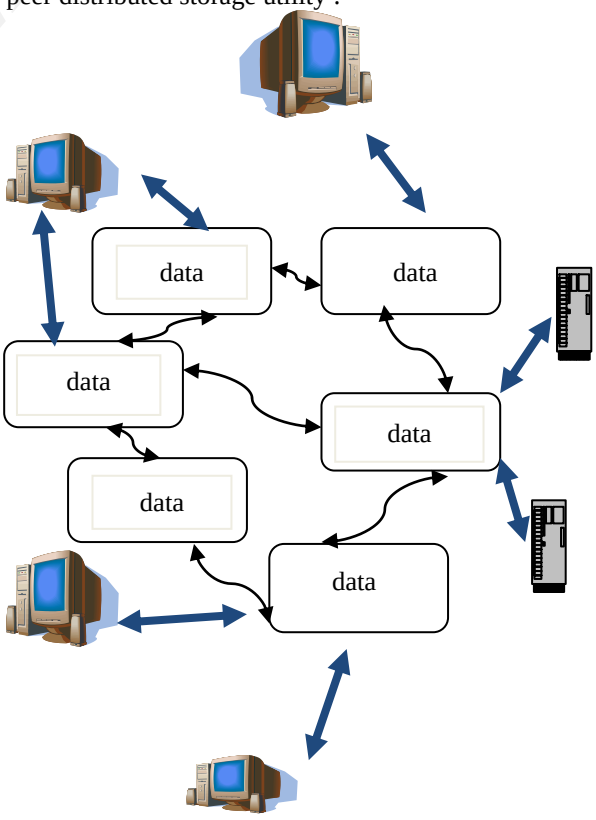

Fig 1. Nomadic data flow

Nodes are not trusted, they may join the system at any time and may silently leave the system without warning. Among the most interesting aspects of PAST's design are (1) the Pastry location and routing scheme, which reliably and accurately routes client requests among the PAST nodes, has excellent properties to identify locality of network and automatically resolves node failures node additions; (2) the use of randomization to ensure diversity in the set of nodes that store a file's replicas and to provide load balancing [2].In this IP address of the nodes (set of nodes which are closer to each other) are maintained by some nodes. When a node wants to forwards data it perform comparison with the field ID of nodes(leaf set),if it finds any similarity the nodes forward otherwise it forward message to the node which is found to be closest to the sender node.

3. Security On Data Storage

Storing data in distributed storage and its management is a tedious task.In Pond: An ocean store Prototype , An OceanStore data object is an analog to a file in a traditional file system. Ordered sequences of data objects which is read-only versions, and in principle every object of all versions is kept forever. Versioning helps to overcome many issues with OceanStore's caching and replication model. As an additional advantage, it allows for time travel, as popularized by Postgres and the Elephant File System ; users can view past versions of a file or directory in order to recover accidently deleted data.[9].directory in order to recover accidentally deleted data.

To provide more security on data stored in cloud and to make it more convenient to the cloud users, key servers with more amenities are introduced .In Plutus:Scalable secure file sharing on untrusted storage, This paper introduces a new secure file system, Plutus, which is capable of providing strong security measures even with an untrusted server. The most important feature of Plutus is that all data is stored as encrypted files and all key distribution is managed in decentralized servers.Cryptographic and key management operations are mostly performed by the clients, and the server experiences only little cryptographic overhead. In this paper they point out the the mechanisms that Plutus uses to provide basic file system security features like detection and prevention of unauthorized data modifications, read and write files accesses are differentiated, and to change users' access privileges.[8].

Attacks on data integrity and durability are of great concern In Glacier: Highly durable, decentralized storage despite massive correlated failures. Attacks on integrity: Since Glacier does not have remote delete or update operations, a malicious attacker can only overwrite fragments that are stored on nodes under his control. However, each fragment holder stores a signed manifest, which includes an authenticator. Using this authenticator, fragment holders can validate any fragments they retrieve and replace them by other fragments if they do not pass the test. Assuming, as is customary, that SHA-1 is second pre-image resistant, generating a second fragment with the same hash value is computationally infeasible.[4]Through public key cryptographic certificates ,trust can be maintained between clients and servers. Farsite manages trust using public-key-cryptographic certificates. A certificate which has been signed using a private key. The important types of certificates are namespace certificates, machine certificates, and user certificates. A namespace certificate is used to associates the root of a file system namespace with a set of machines that also can manage the root metadata. A user's personal public key is associated with user certificate. so that the user identity can be validated for access control. A machine having it's own public key is included in machine certificate., which is used for establishing the validity of the machine as a physically unique resource.[3]

4. Availability and scalability

Cloud computing technology with much functionality is expanding day by day. Usage of new computing methodologies, hardware, and software from different vendors made many advancements in cloud technology, but while adding up all these to the existing scenario, interoperability, scalability and availability are of major concern.

In The Newcastle connection or UNIXes of the world Unite. This paper describes a software subsystem that can be integrated to each of a set of physically interconnected UNIX look-alike or UNIX systems, which can construct a distributed system with many functionalities which cannot be functionally distinguishable at both the user and the program level from a conventional single processor UNIX system. The techniques used are applicable to a different types of both local area networks and wide area networks, and solves all issues related to inter-processor communication, network protocols, etc., to be hidden. In UNIX United each constituent UNIX system has its own named set of users, user password files and user groups, its own system administrator (super-user), etc. Each constituent system will perform authenticating functions by checking user identifier and password of all users who attempts to log in to that system.. It has been found that the functioning and working of a multiprocessing operating system shows similarity to those of a (good) multiprogramming system. What has now become clear from this, as a result of the work on UNIX United, is that this similarity

shown in different functions are extended also to distributed systems. The additional compatibility issue that the designer of homogeneous distributed system wanted to encounter should not be allowed to obscure the continued relevance of much established practice regarding the design of systems with high multiprogramming capability.

In proxy Re-encryption scheme Without knowing plaintext to the proxy the proxy can re-encrypt the already encrypted text with recipient's secret key. In some Improved Re-Encryption Schemes with Applications to Secure Distributed Storage[5].A secure file system is a natural application of proxy re-encryption because the system often assumes a model of untrusted storage. The performance of access control server has been performed under a heavy load. It shows that the proxy re-encryption server can scale up to 1,000 pending requests before exhibiting signs of stress. Proxy re-encryption RPCs are used. This caused server to perform proxy re-encryption and no computation is done on client side. The server is able to sustain 100 re-encryptions/sec until reaching about 1,000 outstanding requests .The server coped up with up to 10,000 outstanding re-encryption requests, quickly spiralled downward thereafter. This shown the scalability of proxy re-encryption scheme.

Table1.1 A comparison of different methodologies used in survey

Reference	Data Routing	Security	Proxy re-encryption
[6]	Data will not flow freely in system	High	Proxy re-encryption is used
[1]	Data is allowed to flow freely	Moderate	Proxy re-encryption is not used
[2]	Data stored in different nodes can flow using randomized routing protocol	High	Proxy re-encryption is not used
[3]	Data routing is performed by analysing hierarchy of nodes.	High	Proxy re-encryption is not used

5. Encryption Schemes

Different encryption schemes are used to ensure security in cloud storage system. Proxy re-encryption schemes used is the most important, useful one. Network traffic can be reduced to great extent with this Proxy re-encryption schemes.In [6] A secure erasure code based cloud storage system with secure data forwarding, decentralized erasure coding and proxy re-encryption scheme has been used. A ciphertext can be transferred by a proxy server under a public key PK_A to a new one under another public key PK_B by using the re-encryption key $RK_{A \rightarrow B}$. The plaintext are not known to the server during transformation. Ateniese et al. proposed some proxy re-encryption methods and applied them to the distributed storage systems. In this approach, messages are encrypted by the owner and then stored in a cloud storage server [5]. When owner wants to send his messages to others, he sends a re-encryption key to the storage server ,then the already encrypted messages are re-encrypted by storage server for the authorized user. Thus, the system is able to attain data confidentiality and supports the data forwarding function and the storage robustness of the system is strengthened by further integration of encryption re-encryption, and encoding.

Encryption of data is done to prevent unauthorized access and modification of the data stored. In oceanstore system[1],they encrypt all data in the system that is not completely public and distribute the encryption key to those users with read permission. To revoke read permission, the owner must request that replicas be deleted or re-encrypted with the new key. A recently-revoked reader is able to read old data from cached copies or from misbehaving servers that fail to delete or re-key; however, this problem is not unique to OceanStore. Even in a conventional system, there is no way to force a reader to forget what has been read. Farsite is a distributed storage system which consists of a set untrusted computers. It provides file systems which are secure and scalable that logically functions as a centralized file server. But the file systems are physically distributed across different computers. When an application modifies, changes the file name, creates, renames, or deletes a file or directory, these updates to metadata are committed. By contacting a directory group, a client randomly generates a authenticator key and divides it into secret shares, which it distributes

among members of the directory group. This key will be unavailable to an attacker because the key is not stored in the local disk after a crash .With this key, client signs each committed update using a message authentication code .(Symmetric-key MACs are much faster than public-key signatures.) When from a crash, the client sends the MAC to the directory group along with the locally committed updates. In a single transaction, before jointly reconstructing the authenticator key, the group members first batch the group of updates, then the batch of updates gets validated, and discard the key. No further updates will be accepted after the reconstructing the key.[3]

6.Conclusion

A survey on security challenges and encryption schemes in cloud computing has been done from different perspectives. Data routing methodologies on different cloud system has been analysed, in which some are reliable routing and some are not reliable. When comparing different encryption schemes used shows that ,it provides additional security enhancements to the system, but complexity of system has been increased a lot. A comparison of different methodologies used are shown in Table 1.1 One of the main advancement in Encryption technology is he introduction of proxy re-encryption which helped to reduce the network traffic.

7.References

[1] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, andB. Zhao, "Oceanstore: An Architecture for Global-Scale Persistent Storage," Proc. Ninth Int'l Conf. Architectural Support forProgramming Languages and Operating Systems (ASPLOS), pp. 190-201, 2000

[2] P. Druschel and A. Rowstron, "PAST: A Large-Scale, Persistent Peer-to-Peer Storage Utility," Proc. Eighth WorkshopHot Topics inOperating System (HotOS VIII), pp. 75-80, 2001.

[3] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R.Chaiken,J.R.Douceur,J.Howell, J.R. Lorch, M. Theimer, and R.Wattenhofer, "Farsite: Federated, Available, and Reliable Storage for anIncompletely Trusted Environment," Proc. Fifth Symp. Operating System Design and Implementation (OSDI), pp. 1-14, 2002.

[4] A. Haeberlen, A. Mislove, and P. Druschel, "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Failures," Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143-158, 2005.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," ACM Trans. Information and System Security,vol. 9, no. 1, pp. 1-30, 2006.

[6] A Secure Erasure Code-Based Cloud Storage System with Secure Data ForwardingHsiao-Ying Lin, Member, IEEE, and Wen-Guey Tzeng, Member, IEEE

[7] D.R. Brownbridge, L.F. Marshall, and B. Randell, "The Newcastle Connection or Unixes of the World Unite!," Software Practice andExperience, vol. 12, no. 12, pp. 1147-1162, 1982.

[8]M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 29-42, 2003

[9] S.C. Rhea, P.R. Eaton, D. Geels, H. Weatherspoon, B.Y. Zhao, andJ. Kubiatowicz, "Pond: The Oceanstore Prototype," Proc. Second USENIX Conf. File and Storage Technologies (FAST), pp. 1-14, 2003