A Survey on Secure and Fault Tolerant Cloud Storage Systems

Li Zhang

College of Information Science and Technology, Jinan University, Guangzhou 510632, China;

zhanglitest1@163.com

Abstract

In recent years, cloud computing service and applications are developing rapidly due to flexibility and low cost. As an important component of cloud computing system, cloud storage is a kind of service providing elastic storage resource and synchronous access based on the remote data servers. Aside from providing colorful and feature-rich applications, cloud storage also brings several fatal security risks in term of the fact that data is not controlled by the owner directly. For cloud storage, the internal data and operations performed are not transparent for the clients of the cloud storage. In this survey, we investigate the topic related to secure and fault tolerant cloud storage systems from the aspects of the classic CIA triad (confidentiality, integrity and availability). Moreover, some other critical parts are also included, such as access control, audit and secure data processing. All in all, this survey provides an overview for the current research status of secure cloud storage.

Keywords

Secure, Fault Tolerant, cloud computing servier.

1. Introduction

In recent years, cloud computing service and applications are developing rapidly due to flexibility and low cost. According to the *The NIST Definition of Cloud Computing*[1], cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. As an important component of cloud computing system, cloud storage is a kind of service providing elastic storage resource and synchronous access based on the remote data servers. From the data owners' perspective, including both individual users and enterprises, storing data remotely in a cloud in a flexible on-demand manner brings appealing benefits: elastic storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, personnel maintenance, and so on[2]. Nowadays, several cloud storage systems have been developed in both academic and commercial fields, such as Amazon Simple Storage Service[3], Dropbox[4] and Hadoop Distributed File System[5].

But cloud storage also brings several security risks for the fact that data is not controlled by the owner directly. The internal data storage and processing on the cloud storage provider are not transparent for outside users. For privacy issues, sensitive data (such as the business financial records or personal health information etc.) must be stored in the form of encryption. But the encrypted data storage format affects data retrieval and processing efficiency for the heavy workloads of encryption and decryption computation. Based on the above facts, cloud storage service leaves several topics and problems for researchers to study.

In this survey, we investigate the topic related to secure and fault tolerant cloud storage systems from the aspects of the classic CIA triad (Confidentiality, Integrity and Availability)[6]. Confidentiality makes sure the data couldn't be accessed without authorization. Integrity protects the data couldn't be modified without authorization or the modification could be detected immediately. The availability make authorized users could utilize the data without limitation.

The rest sections are organized as follows: Section 2 describes the general cloud storage architecture. The confidentiality related topics, especially access control, is presented in Section 3. Section 4 and Section 5 provide Integrity and availability related contents correspondingly. Audit is discussed in the Section 6. Secure data operations and processing are also very important in cloud storage service, which is investigated in Section 7. Section 8 concludes our survey.

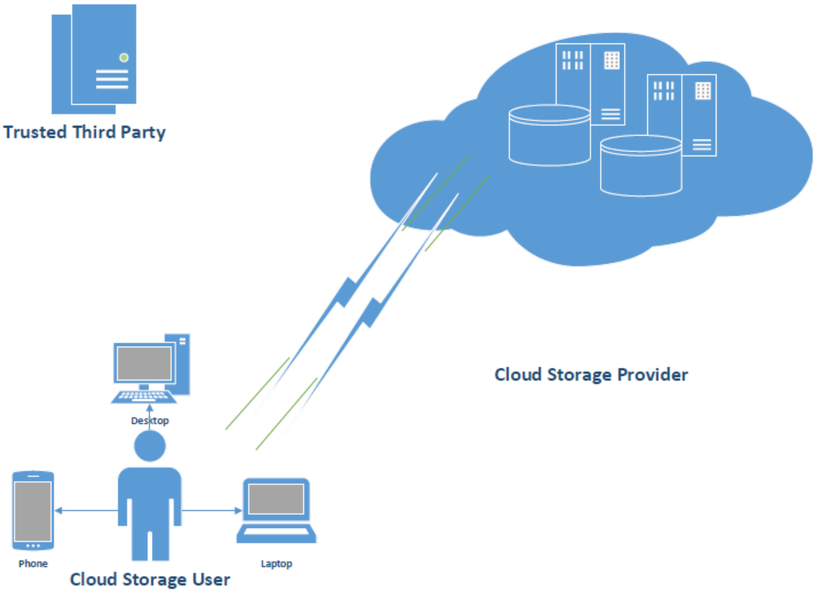

Fig. 1. The architecture of cloud data storage service

2. Cloud Storage Architecture

As described in Fig. 1, the basic cloud storage architecture consists of 2 different entities: cloud storage user and cloud storage provider. The user may be an enterprise customer, who owns several devices, such as desktop, laptop and smart phone. All these devices can access the stored data in the cloud synchronously. On the other side, the service provider not only provides data storage service, but also should make sure data confidentiality, integrity and availability. So the cloud also contains authentication servers, backup servers and other function services.

In some more complex cloud storage architectures, there may exist audit server, key distribution center and other trusted third parties. These advanced topics will be discussed in the following sections.

3. Data Confidentiality

An important requirement of any information management system is to protect information against improper disclosure or modification[7] (known as confidentiality). Access control determines what one party will allow another to do with respect to resources and objects mediated by the former. Access control usually requires authentication as a prerequisite[8].

Traditional access control architectures usually assume the data owner and the servers storing the data are in the same trusted domain, where the servers are fully entrusted as an omniscient reference monitor[9] responsible for defining and enforcing access control policies. However this assumption is not true in cloud storage environment. On one hand, cloud servers are not authorized to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of the owner[10]. So these different features leave several challenges and opportunities for cloud computing researchers.

3.1 User-based Access Control

A simple access control mechanism is user-based access control (UBAC), which is shown in Fig. 2 (part A). In this system, permissions are defined for individual users. The system can accept query "Can user U perform action A on resource R?" and return Yes or No answer. Based on the fact that cloud applications usually contain millions of users and resources, it is difficult to specify policies for every individual tenant on every individual resource. So the original UBAC is not suitable for cloud computing in general. As it is more practical to specify policies relating to groups of entities with similar functionalities. It is helpful to cluster the policies pertaining to the duties of a role within an organization such as a project manager and senior developers[11], that is to say, the role.

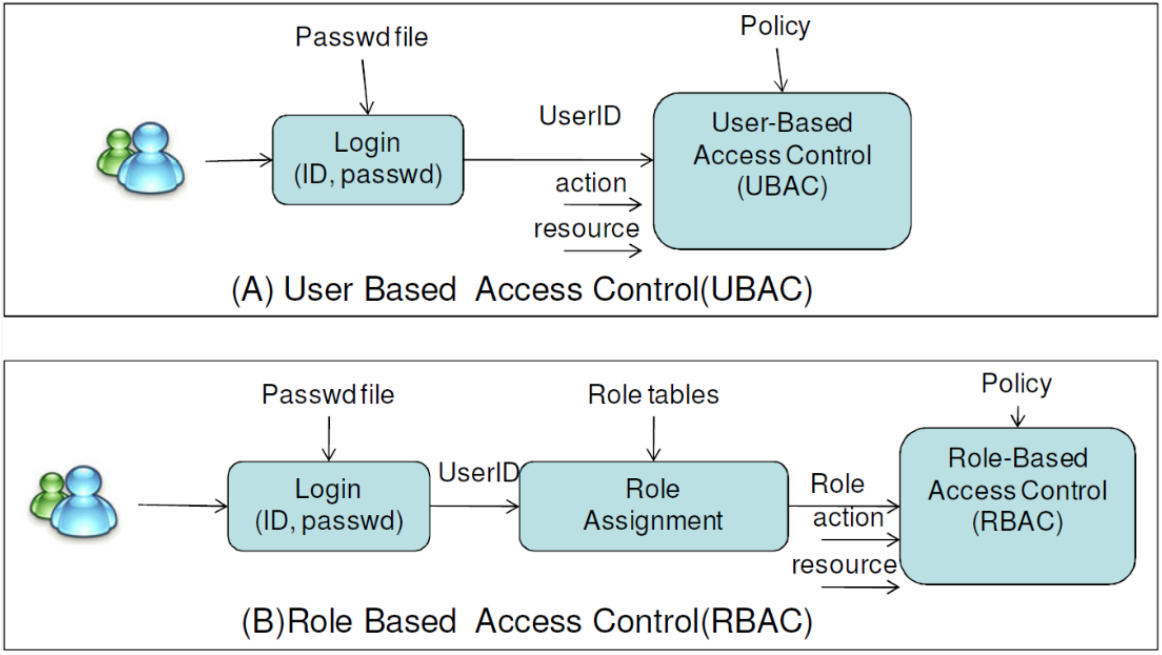

Fig. 2. User Based Access Control(UBAC) vs. Role Based Access Control(RBAC) [11]

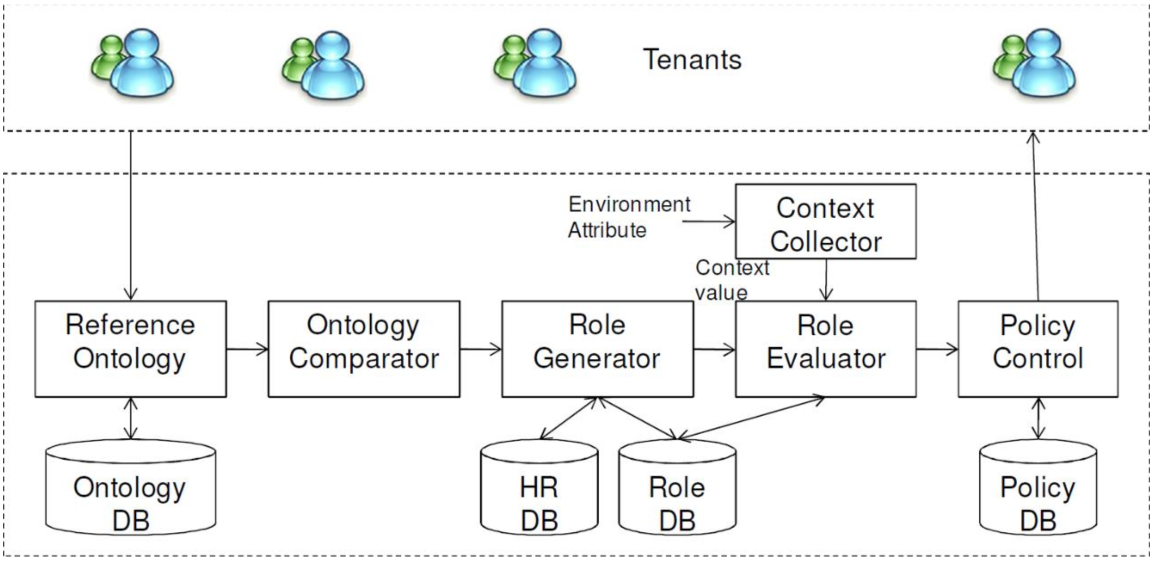

Fig. 3. RBAC using Reference Ontology Framework in Cloud [11]

3.2 Role-based Access Control

Another approach is to use role-based access control (RBAC)[12][13] as shown in Fig. 3 (part B). A role is chiefly a semantic construct forming the basis of access control policy. A typical RBAC system has two phases in assigning a privilege to a user:

In Phase 1, the user is assigned one or more roles. The permission of roles has been pre defined.

In Phase 2, the roles are checked before an operation is executed.

In RBAC, permissions are associated with roles rather than users, thus the permission assignment is not processed for an individual user. Users acquire access rights by their roles, and they can be dynamically re-assigned or removed from roles without changing the permissions associated with roles. The number of roles is typically much smaller than the number of users[11].

Tsai et al. propose a model using a role ontology for Multi-Tenancy Architecture (MTA) in clouds, which is called O-RBAC[11]. Ontology is a conceptual structure which contains knowledge in a domain and their relationships, provides useful and valuable information for cloud computing. The ontology is used to build up the role hierarchy for a specific domain. Ontology transformation operations algorithms are provided to compare the similarity of different ontology. The overall architecture of the proposed model is shown in Fig 3.

When a tenant is trying to access to a protected service/data, the Context Collector module collects various contextual information from both the environment and tenants. The Role Evaluator module uses context information quantify these values and interact with role databases and policy databases to determine the security level. According to the security level, role, and access policy, the Policy Controller determines the appropriate security services, includes granting, denying or revoking access. And then, the result of this security service can be delivered to the service model, and perform actions according to this security checking process[11].

3.3 Attribute-Based Encryption

Attribute-Based Encryption(ABE)[14] is a public key cryptography primitive for one-to-many communications, which could be applied in access control. In ABE, data is associated with attributes for each of which a public key component is defined. The encryptor associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user is assigned an access structure which is usually defined as an access tree over data attributes. User secret key is defined to reflect the access structure so that the user is able to decrypt a ciphertext if and only if the data attributes satisfy his access structure [10].

In the solution of [10], Yu et al. associate each data file with a set of attributes, and assign each user an expressive access structure which is defined over these attributes. To enforce this kind of access control, they utilize ABE to escort data encryption keys of data files. Such a construction enables the solution to immediately enjoy fine-grainedness of access control. In [15], Wang et al. propose a hierarchical attribute-based encryption (HABE) model by combining a hierarchical identity-based encryption (HIBE)[16][17] system and a ciphertext-policy attribute-based encryption (CP-ABE) system, to provide fine-grained access control and full delegation.

4. Data Integrity

In the cloud system, keeping data integrity is a fundamental task [18] for the further operations. The followings are the challenges for data integrity in the cloud storage system.

For the hard disk drivers nowadays, to scale up the data storage in the cloud Computing systems, vendors need to increase the number of hard drives. This may lead to high probability of node failure or disk failure or data corruption.

Disk drives are more and more bigger for their capacity, in turn, this system will not so fast in terms of data access.

4.1 Implementation

Zetta system[19] focuses on the data integrity issues in cloud computing services. It deploys RAIN-6 (Redundant Array of Independent Nodes-6) in its system, which can provide the primary data hosting service, and the data integrity. It has a similar implementation to RAID-6 (Redundant Array of Independent Disks-6)[20], and the two method have similar capability for the cloud storage data integrity.

HAIL[21] manages file integrity by combining the servers or independent storage services together. The storage resources in the HAIL system can be tested and reallocated when failures are detected.

HAIL has a better performance than the basic single-server design of PORs. The system relies on a single trusted verifier, e.g., a client can interact with the servers to verify the integrity of files stored by the client.

4.2 Policy and Protocol

In the opinion of [22], integrity of the cloud infrastructure is ensured through the use of trusted computing, through the powerful combination of remote server integrity and cryptographic protocols, the authors advocate some extension of control from the enterprise into the cloud, the data is protected with the policies deployed, no matter the content lies in the enterprise side or the cloud side[22].

5. Data Availability

Failures are common in current databases, especially more and more data is stored in the database. The availability of cloud storage systems is to guarantee that the users can use them at any time and in any place, which is more complex than common databases. It should be working all the time for any users since the cloud computing system allows the users to access the cloud storage from anywhere. In general, there are two main strategies[18]: hardening and redundancy, used to enhance the availability of the cloud storage and the applications running on the platform.

6. Virtualization

For hardening strategy, many cloud computing system vendors provide the computing platform and cloud storage services based on virtual machines. The famous company Amazon provide EC2 and S3, which are entirely based on the virtual machine Xen, the virtual machine can provide separated memory virtualization, CPU/machine virtualization and storage virtualization etc. The cloud vendors depends on the virtual machines to combine the PCs or servers together, then the vendors can provide a scalable and robust system which have a better availability due to the virtual machines have the ability in providing services in terms of users' individual resource requirement. Therefore, the virtualization technique is the foundation of the cloud services.

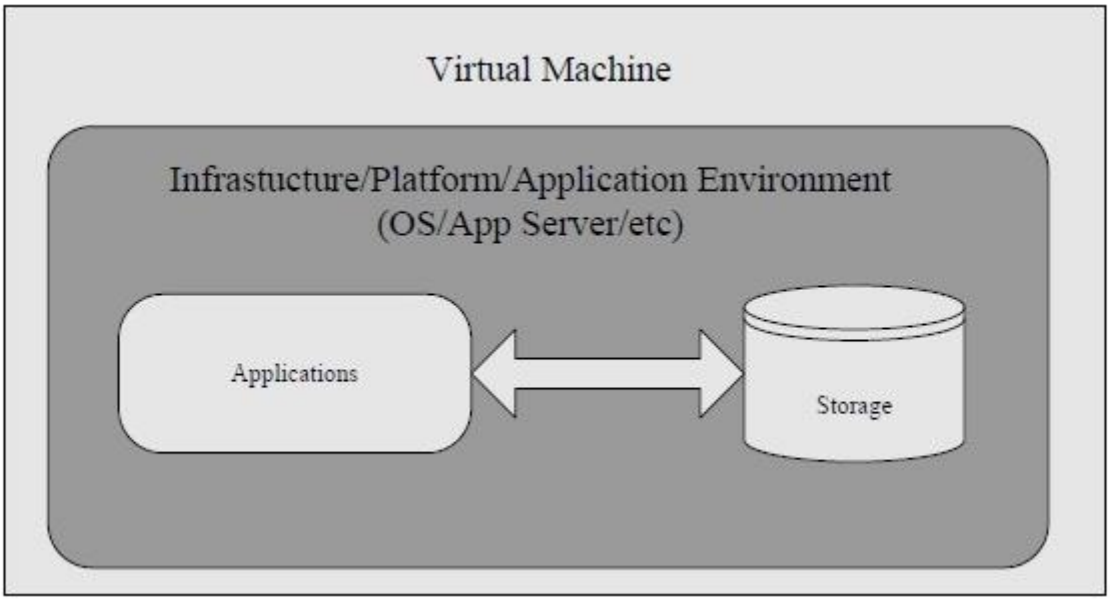

Fig. 4. Virtual Machine as Infrastructure/Platform[18]

As shown in Fig. 4, hosted services lie on the virtual machine, which is combined with a set of CPUs, memory, storage, it is regarded as services' infrastructures or platforms running on. Moreover, the cloud vendors nowadays have the ability to block and filter traffic based on IP address and port which can protect their systems, but these facilities are not the same as the network security controls in the most enterprises.

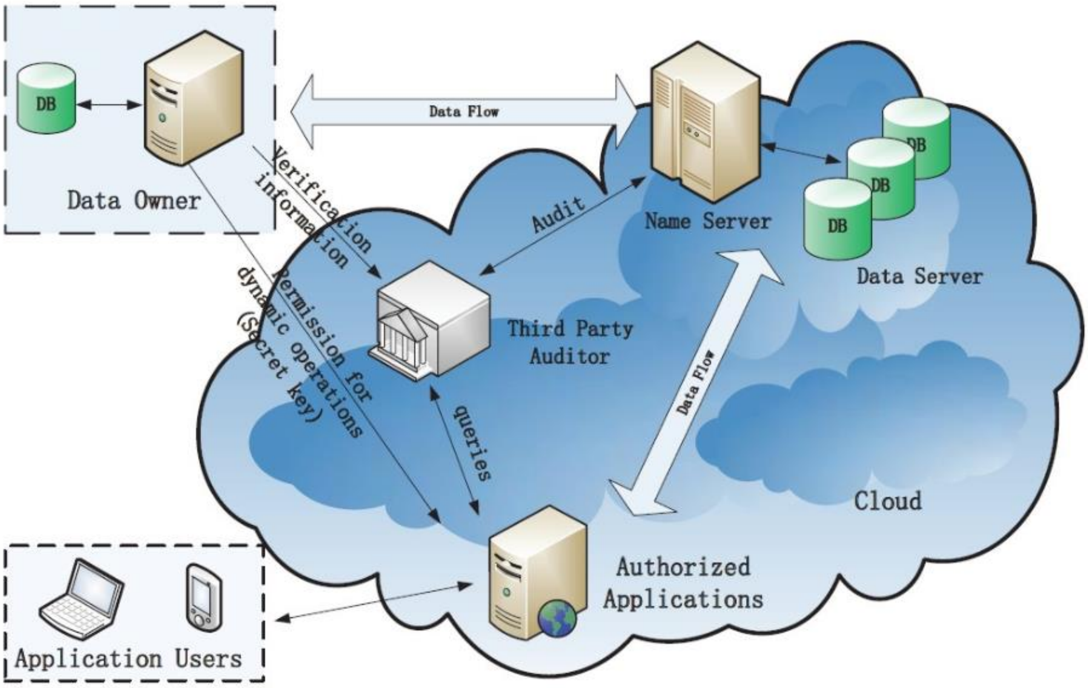

Fig. 5. The Audit System Architecture[29]

6.1 Redundancy

For redundancy strategy, the cloud storage system vendors deploy the geographic redundancy among their cloud systems which can provide high availability. Using instances in separate availability zones, one can protect applications from failure of a single location. The availability zones are distinct locations that are engineered to be insulated from failures in other availability zones and provide inexpensive, low latency network connectivity to other availability zones in the same region. This means the cloud system has the capability to provide redundancy which can enhance the availability.

For example, Google owns more than 1 million machines which are deployed in 36 data centers across the world. Google offers geographic redundancy in its systems. Google file system (GFS)[23] set 3 as the default number of replications for each object it stores. Each file stored in the GFS is replicated at 3 places, which further enhances the availability of the system. Similar to google, Amazon also builds data centers in several regions.One of the most surprising uses of Amazon S3 is content distribution. In this scenario, users use the storage system as distribution points for their data in such a way that one or more producers store the content on their account and a set of consumers read this content.

6.2 Implementation

After discussing the two main strategies to enhance the availability of the cloud storage, we will illustrate some details of the method adopted in real system based on the more detail examples. As we know, the problem about temporary partial unavailability is a well known Internet phenomenon. When the data move, it is inevitable that the system will experienced some unavailability. The denial-of-service attacks will also cause the same problem.

DEPSKY[24] is proposed by Bessani et al., which can handle this problem by using replication and diversity to store the data on several clouds, and allowing the users can access to a subset of the storage. DEPSKY supports dependable updatable information storage even if the content is dynamic distributed and have some security problems. Although many cloud vendors advertise they can provide 5 or 6 nines of availability, the perceived availability in the author's experiments was lower than expected, since the outsourcing storage not only dependent on the provider’s availability, but also on the availability of the Internet. So you need consider twice before you upload your privacy information to the cloud storage.

The HAIL[21] leverages cryptographic protocols to provide a software layer to protect the integrity and availability of the cloud storage, even if the individual clouds are compromised by a malicious and mobile adversary.

The researchers have proposed distributed protocols to check file availability [25], which relies on the clients query across the servers. In this model, a file (defined as F) is typically stored across the redundant and distributed servers. These methods can support files recovery after some failures occur in the cloud computing system.

While for different application or data items, different availability levels may be required. Nicolas Bonvin has proposed their approach that can find the optimal resource allocation dynamically which balances the query processing overhead and also satisfies the availability for different query rates and storage requirements[26].

Skute is designed to provide low response time when the clients do read and write operations on the cloud storage, it can guarantee the geographical dispersion of replications in a cost efficient way and also support different availability levels for different applications, while still minimizing bandwidth and storage consumption of the loud storage. Other approaches, such as [27], the authors claim that they can provide several applications by using a key and value pair store for different applications. Each data item would be independent in [27], an application could severely impact the performance of others if they use the same resources at the same time. To address this problem, Skute allows a fine-grained control of the resources stored, since every virtual node acts as an individual optimizer, Skute can minimize the impact of the applications.

7. Audit

Audit means to take some method to monitor what happened in the cloud storage system[18]. Security audit is an important solution enabling traceback and analysis of any activities including data accesses, security breaches, application activities, and so on. compared to the common audit, the audit service for cloud storages should provide clients with a more efficient proof for verifying the integrity of stored data.

In general, we can add another layer above the virtualized system and deploy some facilities to monitor what happen in the system, this is better than if we only add some monitor code embedded in the application and the software. There are three main attributes should be audited. Event, the instances which affect the system availability; Logs, the information about user's application and the running environment Monitoring, which limit what the vendors need in order to run the facility and it also should not be intrusive. Cloud system developers always focus on providing services based on the virtualized techniques, it means the system can itself entirely. In many countries, they disallow the data and copyrighted material flow outside the country, so finding a way to make the system auditable is important in the law issue perspective.

7.1 Outsourced Data Audit

In order to achieve a rapid implementation and guarantee the assurances of the outsourced data dependability, we need efficient methods that can do data correctness verification.

In [28], Wang et al. propose publicly auditable cloud data storage which will help the cloud economy become more practical. With public auditability, the data owners can get the data information depend on a trusted entity who can act as an audit party to assess the outsourced data. This method can provide a transparent but also cost effective way to help the data owners due to save the owners' computation resources. It sounds good, but to make such a publicly auditable secure cloud storage service become a reality, some critical challenges also need to overcome. The model should not only depend on the cryptographically, but also need to think from a symmetric view.

To minimize the auditing overhead which imposed by the auditing process, the overhead includes many items, such as I/O cost, the bandwidth cost for data transfer and some extra online burden on a data owner. Ideally, the owner should just enjoy the cloud storage service, while do not to worry about storage auditing correctness.

7.2 Dynamic Audit

Dynamic audit services for integrity verification, especailly for the outsourced data storages is a trend for auditing of the cloud system. In [29], the authors proposed a dynamic audit service for verifying the integrity of an untrusted and outsourced storage which constructed based on the following techniques, random sampling, index-hash table, fragment structure, timely abnormal detection and supporting provable updates to outsourced data. Aside from the above method, a probabilistic query and periodic verification for improving the performance of audit services is also proposed by the author. The method will not only validate the effectiveness, but also show the audit system verifies the integrity with lower computation overhead, requiring less extra storage for audit metadata. A proof-of-concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches.

Fig. 5 shows the audit system architecture proposed for the outsourced data in clouds. There are four main entities:

Data owner (DO), who has data stored in the cloud;

Cloud service provider (CSP), who provides data storage service and has enough computation resources;

Third party auditor (TPA), who has capabilities to monitor the outsourced data under the delegation of data owner;

Authorized applications(AA), who has the right to access and manipulate the stored data.

7.3 Secure Data Operation and Processing

In this section, we will focus on secure data operation and processing aspects when users using cloud storage. For privacy issues, sensitive data (such as the business financial records, proprietary research data, or personally identifiable health information etc.) must be stored in the form of encryption. But clients also want to keep the ability of data processing and retrieve segments of their data without decrypting the total data set. These requirements bring the problems of secure data retrieval and secure computation outsourcing.

In this section, we will focus on secure data operation and processing aspects when users using cloud storage. For privacy issues, sensitive data (such as the business financial records, proprietary research data, or personally identifiable health information etc.) must be stored in the form of encryption. But clients also want to keep the ability of data processing and retrieve segments of their data without decrypting the total data set. These requirements bring the problems of secure data retrieval and secure computation outsourcing.

7.4 Secure Data Retrieval

Nowadays more and more data are produced by users. They are motivated to outsource their local complex data management systems to the cloud owing to its greater flexibility and cost-efficiency. Data encryption before outsourcing is the simplest way to protect data privacy and combat unsolicited access in the cloud and beyond[30]. But the user hopes achieve the target that he could query the items without decrypting the total item set. He also could add and delete items dynamically. In the whole processes, the cloud storage provider can't get any information of queried item, respond items and update contents. This problem is so called searchable encryption.

In recent years, several searchable encryption schemes have been proposed. The schemes based on symmetric encryption are adopted widely for more efficiency. SSE-1[31] provides a solution based on <keyword - file list> look-up table. Also they improved the definition of SSE security, that is adaptive security and tuple (*history*, *view*, *trace*). While non-adaptive definitions only guarantee security to clients who generate all their queries at once, adaptive definitions guarantee privacy even to clients who generate queries as a function of previous search outcomes. This definition is extended to controlled disclosure [32] for executing efficiency.

The first dynamic searchable symmetric encryption scheme is proposed in [33], which is designed based on [31] and improves it. The idea is recording extra information for update operations. The delete table and delete array are designed, which are used for recording nodes relationships and keywords set of each file.

7.5 Secure Computation Outsourcing

Despite the tremendous benefits, computation outsourcing to the commercial public cloud is also depriving customers direct control over the systems that consume and produce their data during the computation[25]. However, ordinary data encryption techniques in essence prevent cloud from performing any meaningful operation of the underlying plaintext data[34], making the computation over encrypted data a very hard problem. The operational details inside the cloud are not transparent enough to customers. As a result, there do exist various motivations for cloud server to behave unfaithfully and to return incorrect results, i.e., they may behave beyond the classical semihonest model[35].

In [36] and [37], Atallah et al. give two protocol designs for both secure sequence comparison outsourcing and secure algebraic computation outsourcing, which are based on homomorphic encryptions[38] and/or oblivious transfer[39]. The mechanism design of [28]explicitly decomposes the linear programming (LP) computation outsourcing into public LP solvers running on the cloud and private LP parameters owned by the customer.

8. Discussion and Conclusion

Nowadays, cloud storage service has been deployed and used widely, such as Dropbox and Amazon S3. But the elastic and efficient service also brings several fatal security risks for the fact that data is not controlled by the owner directly. Aside from providing colorful and feature-rich applications, cloud storage also leaves many challenges and problems need to solve and study.

In this survey, we focus on the schemes and techniques for secure and fault tolerant cloud storage systems. The investigation framework follows the classic security definitions, that is to say, confidentiality, integrity and availability. Access control and authentication techniques make sure data confidentiality. The integrity and availability are so critical since they provide the basic support that you can use your any device to access the cloud storage at any time, in any place. The audit service is also important due to it can not only provide clients with a more efficient proof for verifying the integrity of stored data, and also monitor what happen in the cloud storage system. To achieve the ultimate target of data storage, that is processing and application, we also analyze the topics of secure data retrieval and computation outsourcing.

Through the previous sections, many schemes and algorithms have been proposed to secure cloud storage service. Some security problems have been solved partly, but the consolidated standards have not been achieved in both academic and industry fields. How to balance the performance and security in cloud storage is still an open problem for the researchers to study

References

[1] P. Mell and T. Grance, “The nist definition of cloud computing (draft),”NIST special publication, vol. 800, no. 145, p. 7, 2011.

[2] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, “Above the clouds: A berkeley view of cloud computing,” Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, 2009.

[3] A. S3, http://aws.amazon.com/s3/.

[4] Dropbox, https://www.dropbox.com/.

[5] HDFS, http://hadoop.apache.org/.

[6] S. S. Greene, Security Policies and Procedures. New Jersey: Pearson Education, 2006.

[7] R. Sandhu and P. Samarati, “Authentication, access control, and intrusion detection,” The Computer Science and Engineering Handbook, vol. 1, pp. 929–1, 1997.

[8] Sandhu, Ravi and Samarati, Pierangela, “Authentication, access control, and audit,” ACM Computing Surveys (CSUR), vol. 28, no. 1, pp. 241–243, 1996.

[9] J. P. Anderson, “Computer security technology planning study. volume 2,” DTIC Document, Tech. Rep., 1972.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–9.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–9.W.-T. Tsai and Q. Shao, “Role-based access-control using reference ontology in clouds,” in Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on. IEEE, 2011, pp. 121–128.

[12] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Rolebased access control models,” Computer, vol. 29, no. 2, pp. 38–47, 1996.

[13] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, “Proposed nist standard for role-based access control,” ACM Transactions on Information and System Security (TISSEC), vol. 4, no. 3, pp. 224–274, 2001.

[14] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption,” in Advances in Cryptology–EUROCRYPT 2010. Springer, 2010, pp. 62–91.

[15] G.Wang, Q. Liu, and J.Wu, “Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,” in Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010, pp. 735–737.

[16] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in Advances in CryptologyCRYPTO 2001. Springer, 2001, pp. 213–229.

[17] B. Waters, “Efficient identity-based encryption without random oracles,” in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 114–127.

[18] M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, “Security and privacy in cloud computing: A survey,” in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on. IEEE, 2010, pp.105–112.

[19] “Zetta: Enterprise cloud storage on demand.” http://www.zetta.net/.

[20] P. M. Chen, E. K. Lee, G. A. Gibson, R. H. Katz, and D. A. Patterson, “Raid: High-performance, reliable secondary storage,” ACM Computing Surveys (CSUR), vol. 26, no. 2, pp. 145–185, 1994.

[21] K. D. Bowers, A. Juels, and A. Oprea, “Hail: a high-availability and integrity layer for cloud storage,” in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.

[22] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, “Controlling data in the cloud: outsourcing computation without outsourcing control,” in Proceedings of the 2009 ACM workshop on Cloud computing security. ACM, 2009, pp. 85–90.

[23] S. Ghemawat, H. Gobioff, and S.-T. Leung, “The google file system,” in ACM SIGOPS Operating Systems Review, vol. 37, no. 5. ACM, 2003, pp. 29–43.

[24] A. Bessani, M. Correia, B. Quaresma, F. Andr´e, and P. Sousa, “Depsky: dependable and secure storage in a cloud-of-clouds,” in Proceedings of the sixth conference on Computer systems. ACM, 2011, pp. 31–46.

[25] G. Brunette, R. Mogull et al., “Security guidance for critical areas of focus in cloud computing v2. 1,” Cloud Security Alliance, pp. 1–76, 2009.

[26] N. Bonvin, T. G. Papaioannou, and K. Aberer, “A self-organized, fault-tolerant and scalable replication scheme for cloud storage,” in Proceedings of the 1st ACM symposium on Cloud computing. ACM, 2010, pp. 205–216

[27]G. DeCandia, D. Hastorun, M. Jampani, G. Kakulapati, A. Lakshman, A. Pilchin, S. Sivasubramanian, P. Vosshall, and W. Vogels, “Dynamo: amazon’s highly available key-value store,” in SOSP, vol. 7, 2007, pp.205–220.

[28]C. Wang, K. Ren, W. Lou, and J. Li, “Toward publicly auditable secure cloud data storage services,” Network, IEEE, vol. 24, no. 4, pp. 19–24, 2010.

[29]Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, “Dynamic audit services for integrity verification of outsourced storages in clouds,”in Proceedings of the 2011 ACM Symposium on Applied Computing. ACM, 2011, pp. 1550–1557.

[30]K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” Internet Computing, IEEE, vol. 16, no. 1, pp. 69–73, 2012.

[31]R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[32]M. Chase and S. Kamara, “Structured encryption and controlled disclosure,” in Advances in Cryptology-ASIACRYPT 2010. Springer, 2010, pp. 577–594.

[33]S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption,” in Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012, pp. 965–976.

[34]C. Gentry, “Computing arbitrary functions of encrypted data,” Communications of the ACM, vol. 53, no. 3, pp. 97–105, 2010.

[35]C. Wang, K. Ren, and J. Wang, “Secure and practical outsourcing of linear programming in cloud computing,” in INFOCOM, 2011 Proceedings IEEE. IEEE, 2011, pp. 820–828.

[36]M. J. Atallah and J. Li, “Secure outsourcing of sequence comparisons, ”International Journal of Information Security, vol. 4, no. 4, pp. 277–287, 2005.

[37]. Benjamin and M. J. Atallah, “Private and cheating-free outsourcing of algebraic computations,” in Privacy, Security and Trust, 2008. PST’08. Sixth Annual Conference on. IEEE, 2008, pp. 240–245.

[38]P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in Advances in cryptologyEUROCRYPT99. Springer, 1999, pp. 223–238.

[39]S. Even, O. Goldreich, and A. Lempel, “A randomized protocol for signing contracts,” Communications of the ACM, vol. 28, no. 6, pp. 637–647, 1985.