SATBAYEV UNIVERSITY

Computing & Engineering

Volume 1 (2023), Issue 4, 1-5

https://doi.org/10.51301/ce.2023.i4.01

Research on data storage security model and management technology in cloud computing environment

Liu Guohong*

Satbayev University, Almaty, Kazakhstan

**Corresponding author: LiuGuohone@outlook.com*

Abstract. In view of the new challenges that cloud storage services pose to traditional storage technology, particularly in terms of data security, reliability, and management technology, an in-depth study of cloud storage security is crucial, focusing on the basic concepts, structures, and characteristics of cloud storage. Unlike traditional storage, cloud storage operates on a much larger scale as a distributed system, facing unique security risks such as data breaches, unauthorized access, and loss of data integrity. It's imperative to analyze the different structural levels of cloud storage systems, including physical storage servers, network infrastructure, and software applications that manage data distribution and access, as each level presents distinct vulnerabilities requiring tailored security measures like physical hardware protection, advanced encryption, robust authentication mechanisms, and regular security audits. Additionally, the implementation of redundancy systems is essential for maintaining data integrity and availability in case of hardware failure or cyber-attacks. Conclusively, a comprehensive cloud storage security model is proposed, encompassing technological solutions, policy, and governance frameworks to establish guidelines for data privacy, regulatory compliance, and ethical standards, thus ensuring the security and reliability of cloud storage systems and making it a secure, efficient alternative to traditional data storage methods in our increasingly data-driven world.

Keywords: *cloud storage, security model, data storage, access control.*

1. Introduction

Cloud computing represents a model designed for providing and managing an expandable, flexible pool of shared resources, both physical and virtual, across a network. This is achieved through on-demand self-service. Extending and evolving from the concept of cloud computing, cloud storage emerges as a novel idea. It leverages functionalities like cluster applications, grid technologies, or distributed file systems. The core of cloud storage systems is to integrate a vast array of varied storage devices within the network. They operate cohesively through application software, offering combined external data storage and business access services. Nowadays, cloud storage services have gained extensive usage, encompassing a diverse range of services such as network drives, online storage solutions, online backup, and online archiving, all falling under the umbrella of cloud storage services. Concurrently, as the utilization and popularity of various cloud storage services increase, concerns regarding data security, including issues like data alteration, data theft, and data loss, are garnering heightened attention.

2. Cloud storage model

The composition of a cloud storage system is multifaceted, encompassing a variety of components such as networking hardware, storage devices, servers, application software, interfaces for public access, access networks, and client applications. In this architecture, each segment fundamentally relies on storage devices, and these devices, in conjunction with application software, facilitate external data storage and access services for businesses. To the end user, cloud storage doesn't signify a single specific device; rather, it is perceived as an aggregate of several storage devices and various other resources, forming a resource pool. User interaction with cloud storage isn't limited to a particular storage device; instead, it's an engagement with a data access service rendered by the entire system. This perspective categorizes cloud storage fundamentally as a service. The essence of cloud storage lies in its collective storage devices and the application software that converts these devices into functional storage services.

In comparison with traditional storage systems, cloud storage systems exhibit several distinctive features. Firstly, in terms of functionality, cloud storage systems cater to diverse online storage services across networks, whereas traditional systems are designed for high-performance computing, transaction processing, and other specific applications. Secondly, from a performance standpoint, cloud storage services prioritize aspects like data security, reliability, and efficiency. Given their broad service spectrum, large user base, and the complexity and variability of network environments, providing high-quality cloud storage services poses significant technical challenges. Thirdly, concerning data management, cloud storage systems are tasked with offering not just traditional file access, but also managing large-scale data and supporting public service functions for easier management and maintenance of background data in the system. Based on these attributes, we have conceptualized a structural model for cloud storage systems, essentially comprising four layers, as depicted in Figure 1.

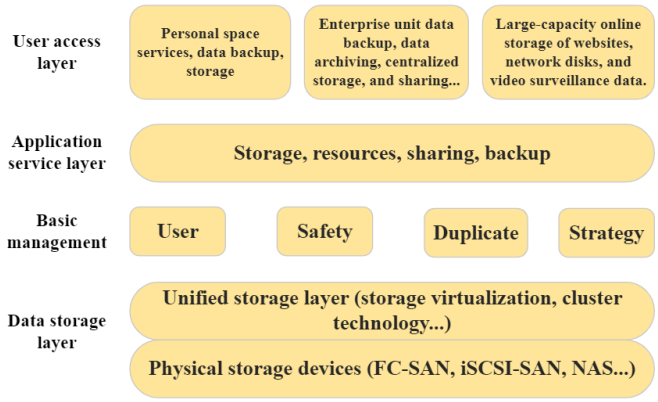

Figure 1. Cloud storage structure model diagram

(1) Data storage layer

At the core of any cloud storage system is its data storage layer. This fundamental component is responsible for linking various types of storage devices, thus enabling the collective management of extensive datasets. Its primary functions include the centralized control of these devices, ongoing status monitoring, and the ability to dynamically adjust storage capacities. Essentially, this layer acts as a service-centric, distributed storage system. The storage devices within this framework might include Fibre Channel (FC) devices or IP-based solutions like iSCSI (Internet Small Computer System Interface) and NAS (Network Attached Storage). Typically, these devices are numerous and spread across diverse locations, connected via wide area networks, the internet, or Fibre Channel networks. This setup ensures that data from different services within the cloud storage system is consistently and uniformly stored, resulting in the formation of a large-scale data repository.

(2) Basic management

The data storage layer holds a pivotal position in the cloud storage system, offering an integrated management perspective across varied services to the higher layers. This layer employs an array of technologies such as clustering, distributed file systems, and grid computing to facilitate seamless connections between multiple storage devices in the cloud, collectively enhancing the performance of diverse external services.

In terms of security at this level, safeguarding data access in cloud storage is achievable through strategies like utilizing content distribution systems and employing data encryption technologies. Concurrently, the implementation of various data backup and disaster recovery techniques plays a crucial role in ensuring the preservation and integrity of data within cloud storage. These measures are also fundamental in maintaining the overall security and stability of the cloud storage system itself.

(3) Application service layer

This layer is the part of the cloud storage system that can be flexibly expanded, faces users directly, and interacts with actual applications. This layer can develop different application service interfaces according to user needs and provide different application services, such as online archiving services, online backup services, and network hard disk services.

(4) User access layer

A networked terminal device anywhere to access the cloud storage system and use cloud storage services according to standard public application interfaces.

2.1. Security of cloud storage

2.1.1. Classification of security levels of cloud storage systems

In the era of cloud computing, a large amount of personal and enterprise data is often no longer stored on their own hard drives. Most of the data is stored in cloud computing operating systems or cloud storage systems through the network. The security and reliability of data will inevitably become a problem for users. A matter of great concern. Since different users in the same cloud computing system have different payment capabilities and different requirements for the security and reliability of their own data, the cloud computing system or cloud storage system should provide different levels of data security for different users. The security decomposition method of cloud storage systems is divided into the following four levels from low to high according to the data storage method and the different requirements of users: stand-alone level, cross-server level, cross- cluster level and cross-data center level. Among them, the stand-alone level means that each data block is only stored on one server. When the server storing the file data blocks fails, the file will be damaged. Cross-server level means that each data block stored will be backed up on different servers. When one of the servers fails, the storage service access will be automatically transferred to other backup databases to ensure data integrity. Cross- cluster level means backing up each data block between different clusters (a cluster contains multiple servers distributed in the same cabinet or different cabinets) to prevent data from being destroyed after the cluster fails. At the same time, since servers in a cluster often share network switching equipment, cross-cluster- level cloud storage systems can overcome the problem of being unable to obtain data once network switching equipment fails, further improving data security. The cross-data center level means that copies of data blocks are stored in data centers in different regions. The physical distance between the two data centers may be thousands of miles. This level of security files can also ensure the integrity of the data in the event of major disasters and accidents. and reliability. Data storage with this level of security is often used in core critical data storage applications such as telecommunications and finance.

In the security level division structure of cloud storage systems, different security levels are generally inherited downwards, that is, cross-data center-level security policies can also implement cross-cluster-level and cross-server-level security policies. The higher the security level of the cloud storage system, the higher the corresponding costs and fees. Users in the cloud storage system can customize storage services of different security levels according to their actual application situations and needs.

2.2. Cloud storage security technology

In cloud storage systems, the safeguarding and dependability of user data within the "cloud" encounter more profound challenges, characterized as follows: Firstly, cloud storage, providing scalable data services, lacks precise security boundaries and defined protection hardware, complicating the development of effective security measures. Secondly, as cloud storage transmits data via IP networks, it inherits common network security threats such as data destruction, theft, alteration, and denial of service attacks, all of which jeopardize data safety. Thirdly, data storage security encompasses both static

and dynamic aspects. Static security focuses on protecting data at rest in the cloud storage system, while dynamic security ensures the integrity and confidentiality of data during transit, with numerous risks involved in securing data dynamically in cloud storage. Fourthly, cloud storage is obliged to maintain data's fault tolerance, recoverability, and integrity, particularly in managing service continuity and avoiding data loss during disasters. Finally, being a public data center, cloud storage systems feature multi-client connectivity, high interactivity, and elevated data security needs. They are highly susceptible to intrusions, attacks, viruses, and malware, necessitating proactive, real-time monitoring and defense of data flows within the cloud storage environment.

Storage security technologies in cloud storage include the following:

(1) Virtual security technology. Virtual technology is a key core technology for realizing cloud computing. Storage resource providers on cloud storage platforms that use virtual technology must provide security and isolation guarantees to their users. Existing research has proposed technologies such as isolation execution machine technology in the Grid environment based on virtual machine technology, performance and security isolation technology based on cache-level aware core allocation and cache partitioning page dyeing methods, etc., so as to improve the basic resources. This layer ensures the security and reliability of data in the cloud storage system.

(2) Data privacy protection. Privacy protection of data in cloud storage involves every stage of the data life cycle. Many existing technologies, such as K-anonymity, graph anonymity and data pre-processing technology, or solutions to ensure user data privacy by integrating centralized information flow control and differential privacy protection technology into the data generation and calculation stages in the cloud, can be used. The security and reliability of user data are guaranteed in the cloud storage system.

(3) Encrypting storage involves securing designated directories and files through encryption before saving them. This process primarily comprises two key elements: the creation and management of user keys, and the encryption and decryption of data utilizing these keys. By implementing robust data encryption storage techniques, the protection of sensitive data's confidentiality during its storage and transmission can be effectively guaranteed.

(4) Data recovery. It refers to the distributed block storage of large key data and multiple backups. When a certain data block fails, the data block can be restored in time and the integration with other data blocks can be completed quickly, making the user feel Failure does not occur. Data recovery can ensure the reliability of data in cloud storage systems.

(5) In cloud storage systems, every application falls under distinct security management domains, with each one governing its local resources and users. Whenever there is a cross-domain resource access by users, it necessitates the establishment of authentication services at the domain's perimeter. This setup is vital for enabling unified identity verification management for those accessing specific resources. In scenarios involving resource access across multiple domains, each domain adheres to its unique access control policy. To ensure resource protection and access, it's imperative to develop a common, mutually accepted access control policy for resources that are shared. Formulating and implementing effective access control policies is crucial in upholding the security and dependability of user data.

(6) Certification services. The authentication service realizes user identity authentication in cloud storage and prevents illegal access and unauthorized access. In the identity authentication of the cloud storage system, the user only needs to prove his or her identity to the cloud storage server. Traditional identity authentication methods often directly expose identity secrets such as passwords, which are easily vulnerable to third-party attacks during the transmission process. In the cloud storage system, the challenge -response authentication method can be used, so that users can prove their identity without sending identity secrets, which improves the security of user data.

(7) Security logs and audits. It is used to record the main security-related activity events of users and cloud storage systems, provide necessary audit information for system administrators to monitor system and user-related activities, and provide certain guarantees for the security and reliability of user data at the application service level. Assure.

2.3. Cloud storage security model

Based on various cloud storage security technologies proposed in 3.2, this paper proposes a cloud storage security model for the cloud storage structural model, as shown in Figure 2. Among them, at the data storage layer, the security and reliability of data in cloud storage are ensured at the physical storage resource level by using virtual security technology, physical security technology, etc.; at the basic management layer, through such methods as data privacy protection, data encryption storage, data Recovery technology and other constructions guarantee the security and reliability of data in cloud storage systems; and at the application service layer, we can use access control, authentication services, security logs and auditing technologies to realize the application of various data in cloud storage. layer security and reliability guarantee.

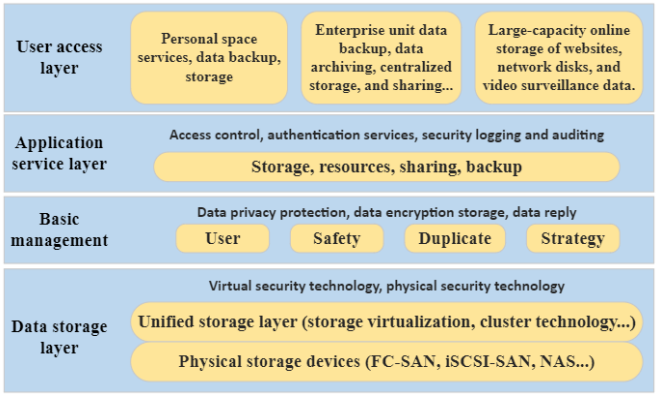

Figure 2. Cloud storage security model diagram

2.4. Current mainstream cloud computing data storage and management technologies

Data storage and management technologies in cloud computing environments cover many aspects such as distributed file systems, object storage technologies, and NoSQL databases. The following is an introduction to the current mainstream cloud computing data storage and management technologies.

1. Distributed file system

A distributed file system is a file system that stores files on multiple servers and accesses and manages them through

a network. In a cloud computing environment, distributed file systems can achieve reliable storage and efficient access of data. Currently popular distributed file systems include Hadoop Distributed File System (HDFS) and Google File System (GFS).

2. Object storage technology

Object storage technology is a data storage technology that stores data as objects. Each object contains data and metadata. Object storage technology supports the storage and access of massive data and provides high reliability and scalability. Currently popular object storage technologies include Amazon S3 and OpenStack Swift

3. Future development trends

With the continuous development and application of cloud computing technology, data storage and management technology are also constantly evolving. In the future, data storage and management technology will continue to develop in a more intelligent, efficient, secure and sustainable direction.

3.1 Integration and development of data storage and management technologies

In the future, data storage and management technology will increasingly develop in the direction of convergence and integration. For example, integrating different types of data storage technologies such as distributed file systems, object storage technologies, and NoSQL databases can achieve more efficient, reliable, and scalable data storage and management. At the same time, data management and analysis will gradually integrate, making data processing more intelligent and efficient.

3.2 Application of artificial intelligence and machine learning in data storage and management

The development of artificial intelligence and machine learning technology will further change the way data is stored and managed. In the future, the data storage system will not only be a simple data storage device, but a data processing platform with intelligent analysis and prediction capabilities. Through artificial intelligence and machine learning technology, the data storage system can automatically identify and classify data, automatically optimize the storage structure, automatically perform data backup and recovery, etc., thereby improving the efficiency of data storage and management.

4. Conclusions

Cloud storage is an emerging industry that is developing very rapidly and has broad development prospects. However, at the same time, it faces unprecedented security technical challenges, which requires researchers in the field of information security to jointly explore solutions. This article proposes a cloud storage security model and management technology that can ensure the security and reliability of user data to a certain extent. But at the same time, we must also note that cloud storage security is not just a technical issue, it also involves many aspects such as regulatory models, standardization, laws and regulations, etc. Therefore, solving the security problem of cloud storage cannot only be done from a technical perspective, but also requires the joint efforts of industry, academia and government departments to achieve it.

References

[1] Laplante, P.A., Zhang, J., Voas, J. (2008). What's in a Name? Distinguishing Between SaaS and SOA. *IT Professional, 10(03), 46-50*

[2] Lin, G., Dasmalchi, G., Zhu, J. (2008). Cloud Computing and IT as a Service: Opportunities and Challenges. *Proceedings of the IEEE 6th International Conference on Web Services (ICWS'08), Los Alamitos, CA, USA*

[3] Wu, Wei. (2019). Research on key technologies of data mining security outsourcing in cloud computing environment. *Changsha: National University of Defense Technology*

[4] Zhang, Hao. (2020). Research on data security issues and protection strategies in cloud computing environment. *Electronic World, (1), 93-94*

[5] Wang, Peng. (2009). Key technologies and application examples of cloud computing. *Beijing: People's Posts and Telecommunications Press*

[6] Feng, Dan. (2009). Research and progress of key network storage technologies. *Mobile Communications, 33(11), 35-39*

Бұлтты есептеу ортасында деректерді сақтау қауіпсіздігі моделі және басқару технологиясы бойынша зерттеулер

Лю Гуохун*

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: LiuGuohone@outlook.com*

Аңдатпа. Бұлтты сақтау қызметтері дәстүрлі сақтау технологиялары үшін, әсіресе деректердің қауіпсіздігі, сенімділігі және басқару технологиялары тұрғысынан туындайтын жаңа мәселелерді ескере отырып, бұлтты сақтаудың негізгі тұжырымдамаларына, құрылымдарына және сипаттамаларына назар аудара отырып, бұлтты сақтау қауіпсіздігін терең зерттеу өте маңызды.бұлтты сақтау. Дәстүрлі жадтан айырмашылығы, бұлтты сақтау таратылған жүйе ретінде әлдеқайда кең ауқымда жұмыс істейді, деректердің бұзылуы, рұқсатсыз кіру және деректердің тұтастығын жоғалту сияқты бірегей қауіпсіздік тәуекелдеріне тап болады. Бұлтты сақтау жүйелерінің әртүрлі құрылымдық деңгейлерін, соның ішінде физикалық сақтау серверлерін, желілік инфрақұрылымды және деректерді тарату мен қол жеткізуді басқаратын бағдарламалық қосымшаларды талдау өте маңызды, өйткені әрбір деңгей физикалық жабдықты қорғау, кеңейтілген шифрлау, сенімді аутентификация механизмдері және тұрақты қауіпсіздік

тексерулері сияқты жеке қауіпсіздік шараларын қажет ететін әртүрлі осалдықтарды көрсетеді. Сонымен қатар, резервтік жүйелерді енгізу аппараттық құралдардың істен шығуы немесе кибершабуылдар кезінде деректердің тұтастығын және қолжетімділігін сақтау үшін өте маңызды. Қорытындылай келе, деректердің құпиялылығы, сәйкестік және этикалық стандарттар бойынша нұсқаулықтарды әзірлеу үшін технологиялық шешімдерді, саясатты және басқару жүйелерін қамтитын бұлттық сақтау қауіпсіздігінің кешенді моделі ұсынылады, осылайша бұлттық сақтау жүйелерінің қауіпсіздігі мен сенімділігін қамтамасыз етеді және оны біздің барған сайын деректерге негізделген әлемде дәстүрлі деректерді сақтау әдістеріне қауіпсіз және тиімді балама етеді.

Негізгі сөздер: *бұлтты сақтау, қауіпсіздік моделі, деректерді сақтау, қатынасты басқару*.

Исследование модели безопасности хранения данных и технологии управления в среде облачных вычислений

Лю Гуохун*

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: LiuGuohone@outlook.com*

Аннотация. Учитывая новые вызовы, которые облачные сервисы хранения данных ставят перед традиционными технологиями хранения, особенно с точки зрения безопасности данных, надежности и технологий управления, крайне важно провести углубленное изучение безопасности облачных хранилищ с уделением особого внимания основным концепциям, структурам и характеристикам облачных хранилищ. В отличие от традиционных хранилищ, облачные хранилища работают в гораздо большем масштабе как распределенная система, сталкиваясь с уникальными рисками безопасности, такими как утечка данных, несанкционированный доступ и потеря целостности данных. Крайне важно проанализировать различные структурные уровни облачных систем хранения данных, включая физические серверы хранения, сетевую инфраструктуру и программные приложения, управляющие распределением данных и доступом к ним, поскольку каждый уровень содержит различные уязвимости, требующие специальных мер безопасности, таких как физическая аппаратная защита, усовершенствованное шифрование, надежные механизмы аутентификации и регулярные проверки безопасности. Кроме того, внедрение систем резервирования имеет важное значение для поддержания целостности и доступности данных в случае аппаратного сбоя или кибератак. В заключение предлагается комплексная модель безопасности облачных хранилищ, включающая технологические решения, политику и механизмы управления для определения принципов конфиденциальности данных, соблюдения нормативных требований и этических стандартов, что обеспечивает безопасность и надежность облачных систем хранения данных и делает их безопасной и эффективной альтернативой традиционным методам хранения данных в наших растущих условиях. мир, основанный на данных.

Ключевые слова: *облачное хранилище, модель безопасности, хранение данных, контроль доступа*.

Received: 14 September 2023
Accepted: 15 December 2023
Available online: 31 December 2023