ATLANTIS PRESS

Advances in Computer Science Research, volume 58

Modeling, Simulation and Optimization Technologies and Applications (MSOTA 2016)

Research on Key Technologies of Multimedia Data Security Protection Based on Cloud Computing

Tingting Yang[1,*] and Shuwen Jia[2]

[1]Institute of Information and Intelligence Engineering, Sanya University, Hainan, China

[2]Teaching Management Office, Sanya University, Hainan, China

[*]Corresponding author

***Abstract*—Cloud computing applications are more widely, with the development of breakthrough at the same time, we should also pay attention to data security, to improve the user's satisfaction. The paper analyzes the key technologies of multimedia data security protection from three aspects: transmission, storage and auditing, including authentication technology, encryption technology, and the construction of audit model and so on.**

Keywords-cloud computing; multimedia data security protection; the identity authentication; encryption

I. INTRODUCTION

Cloud computing which has the characteristics of virtual, universal, large scale, high reliability, has a great advantage in dealing with large data and information exchange and communication based on the Internet technology[1]. At the same time, many companies in the commercial use cloud computing to generate economic benefits, coupled with the characteristics of its virtual and open, so there is a certain risk of cloud computing. For businesses and users, the loss of data or personal information leakage and tampering, consequences are unbearable to contemplate. However, with the development of the Internet these events happened many times, which has caused serious losses to users and enterprises, so how to protect the multimedia data security is very important, and we must strengthen the research of related technology.

II. ANALYSIS OF MULTIMEDIA DATA TRANSMISSION SECURITY PROTECTION TECHNOLOGY

With the popularity of the Internet, the status of cloud data in the life and work of the increasingly important, whether individuals or businesses will often transfer data[2]. In the transmission process, in fact, there is a great risk, which the data once affected that may lead to transmission interruption, or Trojan virus, so that eventually received data become garbled, unable to open source file. In addition, a large number of network transmission channels, but also to ensure the speed, so it is necessary to take effective means to protect the transmission of multimedia data security. These methods contain the user's authentication and authorization, that is, the user login, transmission, encryption, and a series of operations, there should be a corresponding authorization system. These operations cannot be carried out without authentication. The key to the security of multimedia data transmission is encryption, symmetric key system, public key cryptosystem, and so on. In order to satisfy the higher requirements, hybrid encryption technology has attracted more and more attention. This technique has the advantages of two kinds of technologies, such as symmetric cryptography and public key cryptography, which mixed use, and form a new cryptographic algorithm. The private key password can improve the privacy and confidentiality of data, public key cryptography can ensure the integrity of the multimedia data[3].

Identity authentication is the gateway of secure network system, before the user enters the system, at first identification through the identity authentication system and access monitor according to the user identity and authorization permission to access the database determines if the user has access to a resource at the same time, the user request and behavior audit system records, the intrusion detection system for real-time monitoring of whether the invasion behavior. Identity authentication is realized in four ways: password based authentication method, authentication method based on physical documents, authentication method based on biological characteristics and authentication method based on hardware information.

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

III. ANALYSIS OF MULTIMEDIA DATA STORAGE SECURITY PROTECTION TECHNOLOGY

A. Authentication and Encryption

Multimedia data storage mainly refers to the multimedia data information, that is, when the query and application are needed, it can be obtained from the cloud space at any time[4]. Because of the particularity of the network cloud, as well as the huge amount of data, in order to prevent unauthorized interactive accessing, usually people need to log in through the certification after the normal access. Such as common password login, password login and so on, are important means to achieve security defense. Authentication and authorization can be divided into two parts: first, to the tenants as the center, can enhance the user experience; second, to serve as the center, the use of the service right, which can be divided into different

objects, and set the corresponding authentication mode, in order to ensure the security of authentication. It can be practically found that mufti-tenancy technology used more, but with the increase of the number of the tenants, store large amounts of multimedia data to the same medium, hard to avoid can appear holes, cause the conflict between the mixture of multimedia data and the tenant, in order to solve this problem, suggest to build up the RBAC model, based on this to improve mufti-tenant access control scheme[5].

Encryption technology plays an important role in the transmission of multimedia data and the storage of multimedia data. Its principle is the use of data encryption and key management, with the corresponding algorithm, to form the corresponding with the customer password. However, with the development of network technology, more and more people are required to encrypt the encryption technology. Now, it is generally required to encrypt the data with high strength, which will undoubtedly increase the difficulty of storage. In this paper, several potential and practical storage encryption technologies are introduced:

First of all, the homomorphism encryption technology[6]. The technology is developed on the basis of privacy homomorphism. Because in the past if you want to calculate the encrypted data, you must firstly know the decryption function, but privacy homomorphism can omit this step. The encryption function can be divided into some parts of the encryption and the whole encryption, the former refers to the addition of the additive or multiplicative, while the latter refers to both the additive and multiplicative. From the two aspects of function and safety, the technology is excellent, but the study on the current situation, the encryption technology mainly pauses in the theory and in the practical application of the algorithm in the low processing efficiency on the cipher text[7]. We know that cloud computing data security is currently facing a paradox is that if fully encrypted, it will affect the search for the use of cloud data; if not encrypted, it will affect the integrity and security of the data. But the same encryption technology can solve this problem; the main work is to enhance the speed of data processing.

Second, Encryption technology for supporting queries. As mentioned, there is cloud storage paradox, so if you have a support query encryption technology, whether can solve the problem? Related research said, users need to put the conditions of the search query to sent to the server, which is not the secret of the encrypted data at the same time, to search information in the Cloud database, and the final result feedback to the user. But this approach to the query conditions and the requirements of the key word is very strict, must be in accordance with the unified format, but also support the format is limited[8]. This leads to the user after receiving the feedback results, you have to open the file one by one, and the key word relative. In addition, the query server feedback data, probably most of the user is not required, so that the flow of consumption is serious. Someone tried to take a fuzzy query method, but also just to support the Boolean query. For the problem does not support the relevance of queries, but also to take specific measures, mainly the use of correlation and a pair of multi ordered mapping, the whole process of calculating the amount of the query is too large, and the cost is high.

B. Destruction and Isolation

In the business environment, cloud data storage usually set the period of validity, after the expiration of these data is still exist, and the user is no longer stored and used, so it should be deleted. Otherwise, if it is illegal to access, it is likely to lead to leakage of user information, to bring inconvenience. After deleting data exist residue problem, in order to prevent data recovery again, supplier shall ensure previous data completely to clear after users stop using cloud services. Especially some important information and must not be others know. Here it is necessary to search for the third party to supervise and discrimination, but the credibility of the third party and impartiality demand is extremely high, from the point of view of the current reliable technology development degree, there are many problems need to be solved[9].

Isolation technique is an indispensable important part of the data security storage, the nature of cloud computing is a kind of technology architecture of coexistence of multiple users as users more, large data, hard to avoid can appear mistake, cause chaos data storage. Whereas isolation technique isolating each user's data, to ensure the safety in cloud data[10].

C. Compression and Backup

Implantation of Trojan, and malicious hackers attack, can lead to tamper with the cloud user data steeled. For businesses, if critical information is missing, it is bound to bring the heavy losses. Therefore, when using cloud storage service, usually for big data backup, even stored data loss caused by accidents, can enable the backup. Many people even multiple backup, in order to improve the reading speed, in general to be compressed data, but also to reduce the occupied space[11].

IV. Analysis of Security Protection Technology of Multimedia Data Audit

After the user transferring data to the cloud storage space, they often change regularly so as to ensure it the additions and deletions, integrity, accuracy and safety, and it is necessary to record the data, and auditing. If finding data be changed, we do a detailed record; if finding a multimedia data security be risked, we need to promptly remove. Theoretically, the public audit needs to ensure that the user's information security, and support the dynamic change, and the cost to reduce as much as possible, but also to support the batch audit, in order to improve the efficiency of work[12]. In this mainly from two aspects of the data audit security analysis:

First, the status of the data hold. At first, the audit model was built on the basis of the technology of the label audit, although it could protect the privacy of the data effectively, but ignored the dynamic nature of the data. By the static storage of raw material gas, the process becomes more complex, and the process is more complex, and it is easy to have all kinds of problems. With the research in depth, based on the symmetric password mechanism and other factors, and gradually build a dynamic storage model can support the dynamic storage, making the system to calculate the load significantly reduced [13]. The deficiency is that the single server environment, if the use of the process of failure, will cause the data cannot be applied. Even dynamic, not to support all dynamic operations, such as the insertion operation, in this model is difficult to

achieve. When using the model to query the relevant information, it is necessary to set the number of query in advance. Now the data security protection technology has made great progress, research on provable data possession dynamic mechanism is also deepening, with grade certification adjustable table, construct a new audit model is able to safely support the data update. And it supports all dynamic actions; the disadvantage is that the execution efficiency is low.

Second, the integrity of the data. A lot of data is stored in the cloud, each user is very concerned about how to protect the integrity and correctness of the data, and in the past research there have been a number of related technologies. For example, the POR model (data retrieval model, using the evidence) model in data security audit, usually with a model of sampling inspection and error correction code function, maintain data security, in the service period, even if the data is deleted can be restored. In these special data are randomly embedded into the data, and the file encryption, to ensure the information of special data will not leak, but does not support dynamic updating and third party verification. To take a publicly verifiable homomorphism authenticator improved, realizes the disclosure of data recovery, but still does not support dynamic update. After that, some people proposed a method based on homomorphism token and erasure code encoding model makes the construction of audit data, greatly improves the safety performance, but also to quickly find out errors in data server. The token homomorphism in which the role is to maintain the integrity of the stored data. In spite of this, the model also exist obvious shortage, such as the need to be preset number of audit, the computational cost is too big. At present, more and more domestic research in this aspect, but also exist problems, more or less in the future also need to consider more comprehensive, perfecting the audit model, in order to improve data security audit.

V. CONCLUSION

In the information explosion era, cloud computing plays an increasingly prominent role, which the activities will produce relevant data, often and need to upload to the cloud space. With virtual and network cloud and open, in order to ensure the safety of multimedia data, we must strengthen the research of this kind of technology, and qualify innovation and fighting spirit, to rationally use the latest research results, and make cloud computing environment of multimedia data security transmission and storage.

ACKNOWLEDGMENT

This work is supported by natural science fund project of hainan province (project number: 20166235), Sanya branch bureau (project number: 2015YD58).

REFERENCES

[1] Tingting Liu. Research on Key Technologies of Data Security towards Cloud Computing[D].PLA Information Engineering University, 2013.

[2] Xia Wei. Analysis of Date Security Protection Technology for Cloud Computing[J]. Computer Knowledge and Technology, 2015, 21 (1) : 52-53.

[3] Yu Mao. Research on Date Security Protection Technology in Mobile cloud computing [D].Guangdong University of Technology, 2013.

[4] Lijiao zhou. Introduction to cloud computing environment of large data safety and privacy protection [J]. Journal of times report, 2015, 27 (12) : 94.

[5] Ningduo Peng .Research on Key Techniques of Privacy and Date Protection Cloud Computing Environment [D]. University of Electronic Science and Technology of China, 2014.

[6] Peng Sun. Cloud computing oriented data security protection key technologies research [J]. Computer CD software and applications, 2014 (12) : 180.

[7] Kefei Chen, Jian Weng. Data Security and Privacy Protection in Cloud computing[J]. Journal of Hangzhou Normal University(Natural Science Edition), 2014, 25 (6) : 561-570.

[8] Jingyu Wang.Research on Key Technologies of Access Control in Cloud Computing [D].University of Science and Technology Beijing , 2015.

[9] D. A. Keim, F. Mansmann, J. Schneidewind and T. Schreck, “Monitoring Network Traffic with Radial Traffic Analyzer,” in Proc. IEEE Symposium. Visual Analytics Science and Technology, pp. 123-128, 2006.

[10] J. Stange, M. Dörk, J. Landstorfer and R. Wettach, “Visual filter: graphical exploration of network security log files,” in Proc. IEEE Workshop Visualization for Computer Security (VizSEC’14), pp. 41-48, 2014.

[11] Zhangjie Fu, Jiangang Shu, Xingming Sun, Daxing Zhang. Semantic Keyword Search based on Trie over Encrypted Cloud Data, ACM 2nd International Workshop on Security in Cloud Computing (SCC2014), 2014, Pages: 59-62.

[12] Zhangjie Fu, Xingming Sun, Zhihua Xia, Lu Zhou, Jiangang Shu. Multi-keyword Ranked Search Supporting Synonym Query over Encrypted Data in Cloud Computing, IEEE 32nd International Performance Computing and Communications Conference (IPCCC2013), 2013, 1–8, San Diego, CA.

[13] Big data.https://en.wikipedia.org/wiki/Big_data.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[14] Karapisoli E, Sarigiannidis P, Economides A.SRNET:a real-time,cross-based anomaly detection and visualization system for wireless sensor networks[C]. Procedings of the Tenth workshop on visualization for cyber security. USA:association for computing machinery,2013:49-56.