Research on Applications of Cloud Computing in Computer Security Storage

Liuren Wang

Liaoning Police College, Dalian, 116036, China

Abstract: Cloud computing is one of the most popular technologies in information technology development, and the data storage service based on cloud environment is developing fast, which makes more and more enterprises and individuals enjoy the efficiency and convenience brought by cloud storage. But at the same time, cloud storage security issues have attracted the attention of users. This paper expounds the challenges in the security storage of cloud computing in the current stage, and gives the security measures of cloud computing security storage, which provides reference for relevant researchers.

Keywords: Cloud Computing; Security Storage; Data Encryption

1. INTRODUCTION

Cloud computing means that users can get all kinds of services and related resources they need through the Internet, and use services as the mode of use. In terms of technology, cloud computing is the product of the integration of traditional computer technology and network technology, such as distributed computing, parallel computing, utility computing, network storage, virtualization, load balancing and other traditional computer technologies. Cloud computing users can use any type of terminal in any location to access the corresponding application services. Users derive resources from the cloud, rather than the fixed tangible entities in the traditional sense. The resource requested by the user is running somewhere, but the specific location of the application does not need to be understood and not to be feared. Through the Internet, users need only one cell phone or a laptop to get everything they need. Cloud computing is not for a specific class of applications, cloud computing architecture and support can be constructed by rich and colorful, is universal; the scale of cloud is not fixed, with the required dynamic expansion to meet current needs. Cloud computing takes service as its own mode of use, and users obtain their own resources and services through the Internet. It has shocked the information technology field greatly, and the shock has also spread to the field of information security. The development of cloud computing, introduces the topic and new troubles for information security, cloud security issues more and more attention. The cloud security includes access terminal browser security; access terminal security management, customers can not only access, service providers can access; access terminal security authentication. Application services include availability, network attacks, privacy security, multitasking in a virtual machine environment, and so on. Infrastructure layer security includes data security, data location, data integrity and availability, data backup and recovery, security of virtual machines, and so on.

2. DATA SECURITY CHALLENGES FACING CLOUD COMPUTING

(1) Data migration

Data migration is essentially the migration of data associated with the process. Migration data includes not only memory and register dynamic data, but also static data on the disk. In order to let the user can hardly feel down the occurrence of migration must be performed at high speed. In order for the process to resume operation on a new machine, data integrity must be ensured. In addition, if the process is processing confidential data, it must also ensure that the data is not compromised during the migration process. The consumption pricing approach of cloud computing means that the bandwidth is charged per megabyte, and the network facilities are charged by the actual use of CPU and memory resources and recording the increasing storage space. The direct result is that the total cost of cloud computing services is constantly changing every month. When developing a cloud computing environment, don't take it for granted that the level of cloud computing resources you use today is the same as what you will use tomorrow. Such a change will be reflected in the monthly cost of your cloud service. We compare what we have paid with the existing network budget approach, which is already known to cost. The implementation of cloud computing enterprises will need to pay a lot of work to develop systems to facilitate prediction and management of continuous costs. The consumer based pricing approach requires constant monitoring of the consumer to ensure that both the planned cost and the actual cost are correct. The subsequent weekly cost control meeting will be an efficient IT activity that will further enhance services and functionality in other areas.

(2) Data isolation

Data on encrypted disks or data in production databases are important, which can be used to prevent the misuse of malicious cloud service providers,

malicious neighbors, tenants, and certain types of applications. However, static data encryption is more complex, if only the use of simple storage services for long-term file storage, users encrypt their own data, it is feasible to send ciphertext to the cloud data store. However, for PaaS or SaaS applications, data cannot be encrypted, because encrypted data can hinder indexing and searching. So far, there is no commercial algorithm to implement full data encryption. PaaS and SaaS applications to achieve scalability, availability, management, and efficiency. Basically, the multi-tenant model is used, so the data used by cloud computing applications will be mixed with other users' data. Although cloud computing applications have been designed at the beginning, technologies such as illegal access to mixed data have been introduced. Although the security verification tool for some cloud service providers use third parties to review the application or application of third party applications to enhance application security, but because of economic considerations, unable to realize the special data platform of single tenant, so the only viable option is not to any important or sensitive data in the public cloud. Because the shared table architecture to maximize the use of the storage capacity of a single database, so the hardware cost is very low, but the developers, but adds extra complexity, due to multiple customer data coexist in the same database table, so additional logic is required to separate customers data. In addition, the architecture of disaster backup cost is very high, not only need to write code to achieve data backup and recovery in the data, the need for database table delete and insert a lot, once the database table contains other customer data, bring great impact on system performance and other customer experience.

(3) Data remanence

The residual data refers to data after removal of the residual form. The data remains likely to disclose sensitive information inadvertently, so even delete the storage medium data should not be released to the uncontrolled environment such as garbage heap or given to the other third parties. In the cloud application data may lead to a residue the user data is not disclosed to unauthorized party no matter what the cloud, SaaS, PaaS or IaaS are possible. If an unauthorized data leak the user can ask the third party or use third party security tools software platform and application of cloud service providers are verified. So far, no cloud service providers to solve the data problem. The data is the data of residual residue in physical performance is in the form of erased residual, the storage medium are erased may have some things The little data can be reconstructed. In the cloud computing environment, the data of residual are more likely to have no intention of disclosing sensitive information, so the cloud service provider should be able to guarantee the user Xiang Yun storage space where the identification information is released or distributed to other cloud users before completely clear, whether the information is stored in the hard disk or in memory, cloud service providers should ensure that resources where the storage space within the file system, directory and database records to be released or re allocated to other cloud users before completely removed.

3. MAIN APPLICATIONS OF CLOUD COMPUTING IN COMPUTER SECURITY STORAGE

(1) Data encryption

To prevent cloud client data information is stolen, or by internal personnel illegal disclosure, generally access to data using encryption technology. At present, more mature encryption techniques are generally divided into two categories: symmetric encryption algorithm and asymmetric encryption algorithm. The symmetric encryption is to encrypt and decrypt data when using the same key encryption algorithm, the encryption security is not high, but the access speed, the sender needs massive data encryption in general use. In asymmetric encryption algorithms, different keys are used for encryption and decryption, public keys are used for encryption, and private keys are used for decryption. The data transmission can use public key encryption information, but only using the corresponding private key can decrypt the encrypted by the public key information, this encryption security is wise, but the encryption and decryption of the long, slow speed, suitable for a small amount of data encryption. Combining the advantages and disadvantages of the two encryption methods, we can combine the two methods to ensure the security of cloud user data. When the user Xiang Yun server issues a request, the server first generates a RSA public key / private key pair, and then transmits the public key to the user. At this point, the client has to generate its own DES key, RSA public key encryption and use the server to send their DES keys, DES key and sends the encrypted to the server, then the server uses the RSA private key to decrypt the user terminal sends the DES key. So, even if the data is intercepted during transmission, no DES key will not be able to obtain the original data; if the DES key is leaked, the RSA public key encryption and decryption key, still stored on the server, the interceptor is still unable to obtain the original data, this double encryption can greatly enhance the safety of the data.

(2) Identity authentication

Traditional identity authentication is often based on user names and passwords. Faced with the complex application environment and role definition in cloud computing, user name and password as a single security credential cannot meet the security requirements of multiple authentication scenarios in cloud computing. With the increasing cloud customers, cloud storage of data information is also increasing, and if the user's identity was counterfeit,

it is likely to cause data information to be leaked, or malicious change, delete and other consequences. Therefore, when users use cloud storage services, not only through the cloud storage service provider identity authentication, but also follow certain access control policies. Traditional identity authentication with user name and password as a single document has been unable to meet the security needs of cloud customers. Many cloud storage service providers begin to use federated authentication based on various security credentials. Users can first provide the name and password, and then provide the dynamic authentication code provided by the cloud storage service provider, to ensure the legitimacy of user identity. In addition, users provide multiple cloud storage service provider, will produce a lot of passwords, and the use of United identity authentication only need to authenticate once, avoids unnecessary data frequent shuttle block bring clouds. In the security access strategy, we must distinguish between flexible support and dynamic security requirements of different customers, we must first ensure that the strong isolation of cloud data between different clients, so that a user may not be unauthorized access to other users' data; secondly, TO safeguard their own internal cloud customers appropriate resistance data from, for example, enterprise customers can be flexible develop according to their own security needs of access control strategy, internal isolation in different sectors and regions of the data; also can be introduced into the virtual organization, realize data sharing between different users or limit the conflict between the user's data sharing.

(3) Erasure code

In a distributed storage system of computer network, due to the error information location is uncertain and unknown, can use erasure codes, its elements include information symbols, symbols, codes of supervision code, codes and other information, can use erasure codes for three different types: RS erasure codes; no rate encoding; cascaded low-density erasure codes, which can greatly improve the decoding speed, improve the quality and reliability of computer network. Erasure code is the most widely used threshold scheme, and has been applied to both academic and commercial distributed storage systems. The location of error information in error correcting code is usually unknown. We will know that the location error is called deletion error, and the error correcting code is called erasure code. Erasure code is very important in improving the reliability and quality of network communication. The main concepts of erasure codes include information symbols, monitoring symbols, code words, code sets, code spacing, code weight and block codes. The information symbols: refers to the original information before encoding; supervision of symbols: refers to the redundant symbols after error correction encoding in the original information symbols added; codeword consists of information symbols and supervision symbols; code set: a collection of multiple codes with different error correcting encoding information symbols after the formation of the composition; the code distance refers to: between the two codeword distance reflects the number of two codewords corresponding code on different symbols; digital fountain codes are also known as non-rate encoding, the bit rate is not restricted. It has the characteristics of "Fountain": when linear encoding is performed, infinite coded symbol sequences are generated from source symbols, and each coded symbol generated by some independent random source symbols is XOR or generated. The message receiver can retrieve all the source symbols by decoding, simply by receiving the encoded symbol.

4. CONCLUSIONS

Cloud storage services brought by cloud computing bring new data storage mode and resource sharing mode for users, and facilitate people's life and work. But there are many challenges facing the cloud environment, including data migration, data isolation, and data retention. How to ensure the security of cloud storage will be gradually solved with the application of academic research and business circles.

ACKNOWLEDGEMENTS

This paper is the result of General Program of Science Research of Education Department of Liaoning Province in 2015 named “Research on Guidance Model of Urban Transportation Based on Big Data Mining Technology” (Grant No. L2015249).

REFERENCES

[1]Xiong Jun, Design of cloud computing data security storage strategy based on improved secret key, Modern Electronics Technique. Xi’an, 2016, 39(20): 31-34.

[2]Hong Hanshu and Sun Zhixin, Bigdata Storage Security Based on Cloud Computing, Journal of Nanjing University of Posts and Telecommunications (Natural Science). Nanjing, 2014, 34(4): 26-32+56.

[3]Cheng Hai, Anal y sis of Cloud Computing User Data Transmission and Storage Security, Journal of Taiyuan Normal University (Natural Science Edition). Taiyuan, 2015, 14(2): 59-62.

[4]Hua Xiang, Design network security storage system based on cloud computing technology, Application of Electronic Technique. Beijing, 2016, 42(11): 106-107+111.