

A Survey of Cloud Computing and Cloud Security

Xin Sui^{1,a} and Yi Sui^{2,b*}

¹ College of Humanities and Sciences of Northeast Normal University, Changchun,
130117 ,P.R.China

² China Telecom, Beijing Branch Beijing,100124 ,P.R.China

^a Suixin1997@126.com; ^b ericsuiyi@qq.com

Corresponding author

Keywords: Cloud Computing; Users; Cloud Services; Cloud Security; Solutions

Abstract. Cloud computing is a revolution in the information revolution, not just a technological change. With the continuous improvement and development of cloud computing technology, more and more users are using cloud services. At the same time, cloud security has become the first consideration for users. This paper mainly introduces the concept of cloud computing, characteristics, cloud security, and cloud security solutions are discussed.

Cloud Computing

In August 2006, Google CEO first proposed cloud computing, in this search engine conference, using cloud computing to describe Google's service implementation model. Cloud computing applications have received widespread attention from all walks of life, cloud computing models are diverse, and then to meet the various needs of users.

The industry does not have a unified consensus on what is cloud computing. "Cloud" is compared to the Internet, which is used to represent data transmission across the backbone network to the other side of the cloud. Generally there are several classic concepts.

The American Academy of Computer Sciences will provide services and data to different users according to their different needs. This sharing service is called cloud computing. These shared resources, the minimum cost, the fastest speed to provide, as far as possible to reduce the cost of information service providers' management.

The Computer Expert Committee of the Chinese Electronics Society defines cloud computing as a network-based user participation computing model. Cloud computing achieves resource and data interaction through sharing. This computing model is a virtualized, large-scale, dynamic growth of computer resources.

Characteristics of Cloud Computing

Cloud computing has the following characteristics.

Very large-scale: Computer service providers use virtualization technology to spread data information to hosts in different locations, providing efficient and efficient processing capabilities.

Resource pool: the so-called "resource pool" refers to all kinds of software and hardware resources provided by cloud computing. In the process of providing services to users, users do not need to know the working steps of the server, calculation methods, and cannot see the whole working process, just pay as needed.

Rich and high scalability: cloud computing platform can provide diversified cloud products. Cloud computing platform has complex internal structure, large-scale, can continuously expand storage space, processing capacity, to meet the massive needs of users.

Security: Cloud providers use a variety of data protection technology, multiple backups, multi-copy fault-tolerant technology to protect user operations and data security, more secure and reliable than local computers.

Low cost: the automatic management feature of cloud computing reduces the management cost of data center. The commonality of cloud computing volume greatly improves the efficient utilization of IT resources, and cheap nodes can be used to form the cloud.

Advantages of Cloud Computing

Cloud computing provides users with super-powerful computing capabilities, and provides users with unlimited space to store and manage data. Cloud computing can share data and applications between different devices.

Data saved by users on personal computers may be lost because hard disk data cannot be restored, virus invasion, or other human factors. Cloud computing provides users with a safe and reliable data storage center to ensure data security.

Cloud computing providers maximize the use of resources through server virtualization.

Cloud computing must ensure that the fastest and succinct operation meets the needs of users. When a user terminates a service, the corresponding resources should be recovered. Cloud computing platform will dynamically increase and reduce the allocation of resources, and then dynamically manage resources. The operation of automatic resource release and configuration can reduce the overhead cost of marketing.

With the advent of the cloud computing era, the IT industry has gradually transformed into an industrial operation mode with scale effect. Large-scale resource allocation and rational large-scale data centers have replaced a number of smaller individual company-owned data centers. IT industries have gradually changed into a resource-friendly, centralized model, replacing the previous high-energy, decentralized model, and thus optimize the industrial layout.

Problems of "Cloud Security"

Cloud computing brings great opportunities as well as risks. "Cloud security" is an important application of "cloud technology" after "cloud computing" and "cloud storage". It is an extension of the traditional concept of security in the field of IT in the era of cloud computing. "Cloud security" generally has two connotations: first, security cloud, so that security becomes a form of cloud computing services, refers to the network security vendors to build a cloud to provide security services. The two is to create a secure solution through security technology, that is, cloud computing security.

The cloud stores a variety of user data and operational information; users experience the cloud brings a variety of fast, convenient and efficient. The "cloud security" problem is mainly manifested in the following aspects.

In cloud computing platform, users share the entire network through distributed platform, saving data transmission time, reducing the cost of equipment purchasing, building software and hardware environment, and improving the utilization of the entire cloud system. But there are also some problems in this virtual environment, such as the random access of some users; it is difficult to identify the identity of visitors. While sharing the server, it provides a more covert way for the spread of the virus. The client cannot guarantee whether his data information is safe or not. These are all security issues.

To build a cloud computing platform, we need to maintain, develop, invest continuously, and provide a good business model to provide safe and high quality cloud services. Whether cloud providers can provide users with sustained and secure services are also a problem facing cloud computing.

Data center should have enough reliability, data should have backup, and data problems after the response time to solve problems, data fault tolerance. Data security is the core issue of cloud security.

Users are more concerned about the security and confidentiality of data acquisition. Users do a variety of operations through the cloud computing platform, some will cause user data modification or deletion, some of these illegal operations are unrecoverable, or even destructive.

Cloud service is to provide users with efficient processing, data transmission, and sometimes some small omissions may be hacked, security measures must be in place to prevent data loss.

The primary task of cloud security is to determine the legality of user identity. If the hacker obtains the user's login information, he will steal the identity to illegally log in and obtain the customer's data information. It may cause corporate secrets to leak out and cause huge losses.

In short, cloud computing security from the platform, mainly refers to whether the platform itself is safe, reliable, whether it can provide the right services. From the aspect of data storage, it mainly refers to whether the data of the platform is damaged or leaked. Cloud computing security issues mainly come from two aspects, on the one hand, cloud service providers adopt data encryption, authentication, access control measures to protect. On the other hand, it controls and prevents cloud service providers.

Cloud Security Solutions

PaaS application security mainly has two aspects: the application security of customers on the platform and the security of the platform itself. In the platform as a service mode, the isolation mode of multi-user application is the most important principle. In a basic Cloud Architecture, it is almost impossible to ensure safe operation if it is just configured by default. Therefore, the application security configuration process should be well known and the default security configuration should be changed. Install the correct configuration application and its patch in time.

Cloud service providers regard the specific application of users as transparent, and customers should ensure their own safety.

Software as a service refers to the cloud service provider to maintain and manage the overall operation of the system. The cloud service provider should provide data security and application security to customers to the greatest extent. For cloud users, only application layer security functions are required.

The above three points refer to the safety of open platform construction.

Enhancing software as a service application management should strengthen the user login information management, password is the most common method, should use a strong, complex password, and modify the password regularly. Cloud providers strengthen the management of user information, mainly including user access control rights, authentication information, minimum privilege management should be implemented to eliminate the internal factors threatening cloud security.

For cloud users, they should also ensure the safety of their own computers. Cloud users should install anti-virus software, firewall and so on.

The application software installed by the client may have vulnerabilities. These vulnerabilities increase the risk of cloud users being attacked, protect their browsers, update and upgrade in time to ensure the security of the server to the client in the cloud environment.

Conclusion

Cloud computing era has come, to ensure the security of cloud computing, but also involves many technical, policy issues. To solve the problem of cloud security, we must constantly improve the standards of data protection and data storage.

In the future cloud security system, the security protection of users will be more perfect.

Acknowledgements

2018 Jilin Province Education Department "Thirteen-Five" Science and Technology Project "Enterprise Private Cloud Construction Design and Research ", Project No.: JJKH20181306KJ.

References

- [1] Wang Yu Ding. Overview of cloud computing access control technology [J]. software journal, 2015,26 (05): 1129-1150.
- [2] Qin Rong Sheng. The impact of big data and cloud computing technology on auditing. [J]. audit research, 2014 (06): 23-28.
- [3] Zhang Yuqing. Cloud computing environment security overview [J]. software journal, 2016,27 (06): 1328-1348.
- [4] Yang Qingfeng. Key technology prediction and strategic choice in cloud computing era [J]. Journal of Chinese Academy of Sciences, 2015,30(02).
- [5] Wu Kaifeng. Large data analysis technology and application based on cloud computing [J]. China Electric Power, 2015,48(02): 111-116+127.
- [6] Yu Xiaoshan. Cloud Computing Data Center Optical Interconnection Network: Research Status and Trends [J]. Journal of Computer Science, 2015, 38 (10): 1924-1945.
- [7] Wang Qiang. Data Placement and Task Scheduling Algorithm in Cloud Computing [J]. Computer Research and Development, 2014, 51 (11): 2416-2426.
- [8] Wang Binfeng. Overview of Network Design of Cloud Computing Data Center [J]. Computer Research and Development, 2016,53(09): 2085-2106.