Research on Virtualization Security Technology in Cloud Computing Environment

Liang Hao[a], Bo Li[b], Kai Li[c], and Ruosi Cheng[d]

Luoyang Electronic Equipment Test Center, Luoyang 471003, China

[a]haoliangoorr@163.com, [b]boris_lee@163.com, [c]731601979@qq.com, [d]ruosi@126.com

Keywords: Cloud computing, virtualization security technology, attack principle.

Abstract: As a fusion of multiple technologies, cloud computing virtualization technology brought new security challenges to cloud resource management and data privacy protection. This paper studied existing cloud computing the attack types from five aspects of cloud virtualization security technology, and made a cloud platform security analysis on the aspects of ensuring the availability of cloud computing services, confidentiality and reliability of data, and privacy protection. The attack instances, attack principles, attack effects, representative defense schemes, and limitations of existing research were also analyzed and compared to provide security for the healthy and sustainable development of cloud computing.

1. Introduction

Cloud computing greatly facilitates people's life[1]. However, with the wide use of the cloud computing, the virtual security problem of cloud environment is becoming more and more serious, which has become an important factor affecting the development of cloud computing[2-4].

The cloud environment is highly dynamic and resource-virtualized. The cloud system runs with the creation, destruction, and migration of virtual resources. Hence the traditional network security monitoring architecture cannot meet the needs of the existing cloud environment. The feature of the resource virtualization, high dynamics, and sharing makes the cloud environment more vulnerable to attack than traditional networks[5]. So the cloud environment not only faces all the security threats faced by the traditional network environment, it still needs to face many new unknown threats[6]. Therefore, the research on cloud computing virtualization technology has important theoretical and practical significance. It will help to improve the adaptability and the availability of the cloud environment network security monitoring system and provide cloud system administrators and users with an effective means to understand the security status of the cloud environment and secure the network security of the cloud environment.

Based on the analysis of virtualization technology architecture in cloud computing, this paper expounded the threats of virtualization technology from five aspects: virtualized hardware security technology, virtualized middleware security technology, virtualized software security technology, virtualized data security technology, and virtualized application security technology. The corresponding security measures were given ultimately.

2. Cloud virtualized architecture

The virtualization technology abstracts the underlying architecture such as physical resources, making the differences and compatibility between hardware devices transparent to the upper-layer applications, thereby achieving unified management of the underlying resources of the cloud. Virtualization technology is a method of deploying computing resources, which can isolate the hardware, software, data, network, storage, etc. of different levels of the application system. Thereby it can break the division among the data center, network, server, data, application and storage in the physical devices, which enables unified management and dynamic use of physical resources and virtual resources and improves the flexibility and flexibility of the system structure.

The integration of existing computing technologies in cloud computing platforms is achieved through cloud virtualization. The cloud virtualization software divides the physical computing devices into one or more virtual machines, and the user can flexibly configure the virtual machine to perform the required computing tasks. For example, operating system virtualization allows for the creation of scalable virtual systems between multiple computing devices that are independent of each other, while idle computing resources are reallocated, saving computational costs and increasing resource utilization.

As the core technology of cloud computing, the security of cloud virtualization is very important. This paper focuses on cloud virtualization security, as well as various known security attacks and their existing defense technologies. For example, stealing service attacks can illegally steal other people's cloud computing resources. Malicious code injection attacks, cross-virtual side channel attacks, directed shared memory attacks, and virtual machine rollback attacks can cause sensitive information to be leaked or unauthorized access to private cloud resources. The virtualization technology architecture in cloud computing established in this paper is shown in Fig. 1.

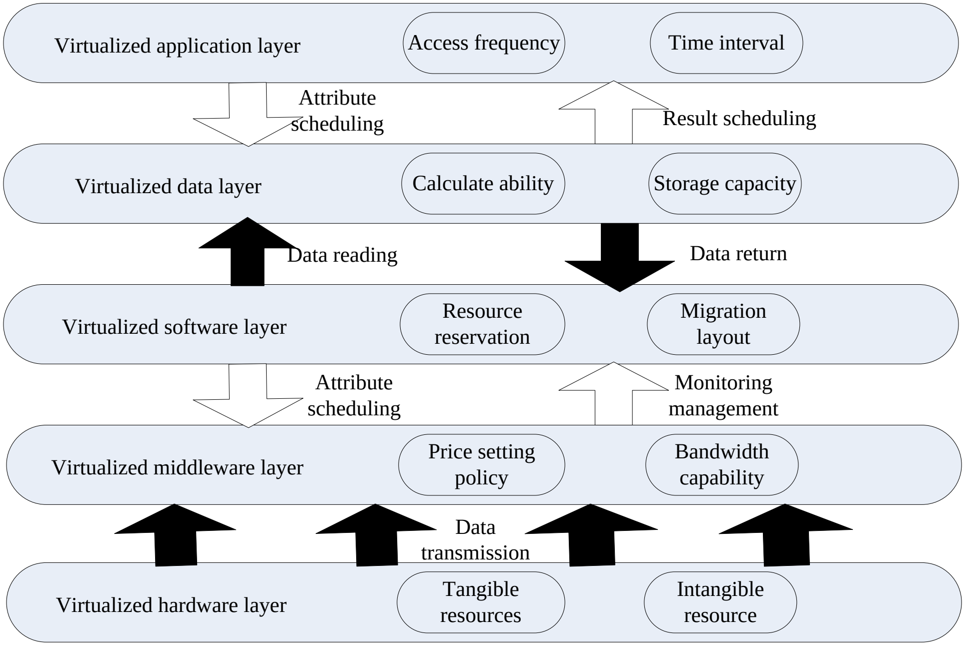

Fig. 1 Virtualization technology architecture in cloud computing

In Fig. 1, the white lines represent scheduled transmissions; the black lines represent data transmissions. The virtualized hardware layer passes the data to the virtualization middle tier. The virtual machine monitoring software allows multiple operating systems and applications to share hardware devices. It is an intermediate software layer running between the underlying virtualized hardware devices and the operating system. The virtualized application layer implements scheduling and use of the software layer by reading data of the data layer.

3. Virtualization security technology and protection

Virtualization security technology protects the security of a single virtual machine, including virtualized hardware security technology, virtualized middleware security technology, virtualized software security technology, virtualized data security technology, and virtualized application security technology.

When implementing security protection for virtual machines, the firewalls and IDS are installed on virtual machines traditionally, but this will result in a large waste of resources. One of the popular methods is to enable a dedicated virtual machine in the virtualization system to provide security protection services for other service virtual machines by deploying independent security functions such as firewall, intrusion detection, and virus protection on the virtual machine. Another way is to install a firewall in the virtual middleware.

To implement the isolation between virtual machines, the virtual machines can be classified based on service attributes, service security levels, and network attributes. The virtual machine can be isolated by the destination IP, source and destination ports, protocols, resource pools, folders, containers, and so on. it can also be isolated from smaller granularities, such as user identity, service type. It can also be isolated through different IP network segments of the VLAN.

3.1 Virtualized hardware security technology

Cloud computing distributes information resources and data computing exchanges on a large number of networked computers. Users access the storage system and networked computers on demand to obtain information exchange and massive data computing functions. The cloud computing model exposes resources and data that were originally confined to the internal network to public networks. The attacker accesses the cloud hardware device physically, and modifying the source program of the virtual machine and changing its function by executing the malicious program code, the purpose of attacking the virtual machine can be achieved.

Hardware device security is an indispensable part of cloud infrastructure security. Instantaneous hardware failures or errors can jeopardize the correctness and security of the overall information system. Different from traditional software security technologies, the introduction of hardware systems brings a new security protection strategy to cloud computing. The hardware security module is responsible for storing and managing private keys for authentication and encryption. It has a high encryption and decryption operation speed and security level, and is easy to integrate with other network devices.

The development of hardware security is limited to a certain extent by low cost performance. In order to overcome the limitations of hardware security in terms of flexibility and scalability, it is inclined to use software architecture instead of hardware equipment to obtain better service capabilities. Therefore, the service reliability improvement of hardware security will bring more opportunities for users to save computing costs. The hardware-based identity authentication mechanism protects data security by embedding security policies into hardware modules, so that it allows users to outsource more data to the cloud while ensuring privacy, which reduces user security and computational overhead overall.

3.2 Virtualized middleware security technology

Virtualized middleware is located between the virtualized resource pool layer and the virtual machine layer. It manages the operation and maintenance of virtual machines, allocates resources, and manages the virtual and abstraction of hardware devices. Therefore, the virtualized middleware security technology is especially important. The main security technologies are Hypervisor own protection technology and virtual firewall technology.

Hypervisor own protection technology can be achieved by building lightweight Hypervisor and the integrity protection. As the function of Hypervisor increases, the volume increases and the credibility decreases. The problem of Hypervisor code problems is solved by simplifying functionality, and building Hypervisor with lightweight virtualization architecture, which are the effective measures for building a lightweight Hypervisor. By using trusted computing technology, integrity metrics and integrity verification of Hypervisor, Hypervisor's integrity protection can be achieved. It enhances the security and credibility of the virtualization platform effectively.

Due to the existence of virtualization technology, the boundaries between virtual machines disappear, and the communication between virtual machines is directly completed between virtual machines, and the security of data exchanged cannot be checked by the outside world. Virtual firewall technology is an effective way to solve this problem. This kind of firewall is a software firewall running in Hypervisor. When communicating between virtual machines, the data is forwarded by Hypervisor. Before forwarding, Hypervisor software firewall filters and monitors the data. The security is guaranteed.

3.3 Virtualized software security technology

The virtualized machine software security technology mainly refers to the security technology used to ensure data security during the operation of the virtual machine. Virtualized software security technology enables resource reuse and improves service availability. In some server failures, the virtualized software security technology can automatically switch services to other virtual servers in the same environment to achieve business continuity. The virtualized software security technology can also use a server to replace the previous multiple servers, which was conducive to cost savings and improve resource utilization. The virtualized software security technology must ensure the security of the virtual machine migration process. The encryption technology can be used to encrypt the migrated objects. In addition, the security configuration environment must be consistent before and after the migration, so that the virtual machine can run normally after migration. The virtualized machine software security technologies include the following.

The virtual machine rollback attack. In the cloud virtualization environment, the management program can suspend the virtual machine and save the system state snapshot at any time for the purpose of normal system maintenance. If the attacker restores the snapshot illegally, a series of security risks will be caused, and the historical data will be cleared, the attack will be completely hidden.

Stealing service attacks. Public cloud computing environments employ multiple flexible billing models typically. However, the periodic sampling of the charging mode and the low precision clock scheduling strategy enable the attacker to exploit the vulnerability of the virtual layer scheduling mechanism, which causing the management program to detect the CPU or VM erroneously. It is the stealing service attack. The specific method is to ensure that the attacker process is not scheduled when the scheduler counts, thus occupying other people's cloud service resources in a hidden way. The conventional virtual machine scheduling mechanism does not check the correctness of the scheduling, which is the main reason for stealing service attacks.

Malicious code injection attacks. The malicious code injection attack uses a malicious instance to replace a system service instance to process a normal service request, thereby the privileged access, illegally stealing certificate information or user data can be gained. Unlike traditional web applications, cloud computing environments are virtualized. The features intensify the security threat of malicious code injection attacks. The operation of cloud service migration and virtual machine coexistence makes the detection of malicious code extremely difficult. Currently, there is still a lack of effective checking methods for cloud service instance integrity. The key point of existing defense solutions is the detection of a compute node that contains a malicious instance.

Directed shared memory attacks. The targeted shared memory attacks target the shared memory or cache of a physical machine or virtual machine. It is the basis of malicious code injection attacks and side channel attacks. It can combine internal attacks to access virtual machine memory to dump data, which may result in the current operating status of the system or the leakage of user privacy information.

Cross virtual machine side channel attacks. The attack is a common form of access-driven attack. It requires the attacker to use the same physical layer hardware as the target virtual machine. The two are alternately executed. In the process of alternating execution, it can be inferred the behavior of the target virtual machine, and the information of the server host. Firstly, The attacker accesses the shared hardware and cache by means of the malicious virtual machine, and then performs predetermined security attacks, such as a side channel attack, an energy-consuming side channel attack, and a high-speed hidden channel, Which lead to the leakage of user data in the target virtual machine eventually. Such attacks are generally difficult to leave traces or trigger an alarm, so they can evade detection. Specifically, the channel attack measures the execution time of different computing tasks, the identity information of the user and the server can be successfully obtained . The side channel attack of energy consumption uses the energy consumption log to attack, which can help the attacker to quickly identify the type of the target virtual machine management program.

At present, the typical defense strategy for the attack is key distribution mechanism and minimum runtime guarantee mechanism. The former divides the user key into random shares and stores each key share in different virtual machines in a periodic update. The virtual machine can guard against the attack behavior of stealing the encryption key effectively by using the cross-virtual machine side channel attack. The latter optimizes the virtual machine scheduling mechanism to reduce the security risk of the cache sharing, and stipulates that the CPU resource cannot be pre-occupied within the minimum running time limit.

3.4 Virtualized data security technology

Cloud computing is different from the traditional computing mode, the ownership and control of user privacy data are forced to be separated from each other. As the core service provided by cloud computing, Cloud storage is a solution for sharing data between different terminal devices. Data security has become one of the key challenges of cloud security, and it has a large proportion in recent research.

The related issues of data security and content privacy protection in cloud computing environments are studied in this paper. So far, the common method of protecting cloud data security is to encrypt the data stored in the cloud server in advance, and decryption it when needed. In this process, the proxy re-encryption algorithm and the attribute encryption algorithm are used to resolve the identity difference between the data owner and the user. the access control technology is used to manage the authorized access scope of the resource. The searchable encryption technology implements the retrieval of secret text data. Finally, in order to prevent user data loss caused by CSP system failure, it is necessary to provide proof of data integrity and ownership. Virtualized data security is mainly reflected in data sharing algorithm, access authority authentication, secret text search and integrity audit, etc., which mainly include data encryption technology, data isolation technology, data backup technology and data clearing technology.

The data encryption technology includes the symmetric encryption technology and the asymmetric encryption technology. The Symmetric encryption technology is faster and more efficient than asymmetric encryption. However, a secure channel must be established to exchange symmetric keys before encryption. Nowadays, the combination of symmetric encryption and asymmetric encryption are generally used to encrypt during the communication process. At present, a CA-based security infrastructure is generally established, and the functions such as encryption, signature, and authentication are handed over to independent components to achieve high efficiency.

There are three mature solutions in the specific implementation of data isolation technology. The first mature is the shared table isolation architecture. The same database instance and database table are shared by users, but the data is separated by fields such as IDs in the database table. The second mature is the separation table isolation architecture; users share the same database instance. but different users' data is stored in different tables in the database. The third mature is separate the database isolation architecture, user data is stored in different database instances to achieve isolation.

The data backup technology balances data security and usage efficiency by designing a dedicated backup strategy. In a practical application, the first copy of the data is stored on a different disk on the same server, the second copy is stored on a different server in the same rack, and the third copy is stored on a different server in a different machine room. When the application is accessed, the required data can be obtained at the fastest average speed, and the backup of the data can be ensured to the maximum extent.

The data clearing technology is mainly to prevent leakage of residual information. Due to the characteristics of resource sharing in cloud computing, the same storage resource may be repeatedly used by different users. If the previous user does not clear the data before releasing the resource, or the cleaning is not complete, the next user assigned to the resource easily restores other people's data information. The data clearing technology uses a mechanism such as disk erasing and data destruction algorithms to forcefully clear data when the user releases the resources, and then allocate the resources to other users.

3.5 Virtualized application security technology

The security of virtualized applications is especially important. It directly related to the future development of the cloud computing industry. For cloud-based applications, such as web operating systems, database management systems, data mining algorithm outsourcing agreements, it is necessary to prevent the inherent security vulnerabilities of the application itself, while the targeted security and privacy protection solutions are designed to improve application security. The security threats of cloud computing applications faced at the technical level are analyzed in this paper, including denial of service attacks, bonnet attacks and audio steganography attacks. Virtualized application security technologies mainly include trusted access control technology, secure access technology, and multi-tenant isolation technology.

When cloud computing users use cloud services provided by service providers, the security and legality of their own behaviors are not guaranteed. To ensure that Cloud computing system security, service providers need to use trusted access control technology to judge user credibility, and formulate corresponding access control rules accordingly. The trusted access control technology calculates the trusted value of the determined object based on the trust level of the user behavior, and assigns the corresponding role and authority according to the trusted value. In the normal dynamic trusted access control scenario, the user's trust level and the role permissions are dynamically changed. The role assignment and permission adjustment are based on the trust level. The change of the user trust level will bring about changes in the role permissions, which regulates user behavior and ensure the security of the cloud computing platform.

From the view of users, the secure access technology ensures that legitimate users can access the cloud computing platform securely and efficiently to obtain the required services. From the perspective of the cloud platform, the secure access technology ensures that the cloud platform is not accessed and attacked by illegal users. The security access technology mainly solves the problems of identity management, password and authentication management, access authorization, auditing, etc. The key technologies involved are single sign-on technology and API protection technologies.

In the single sign-on technology environment, cloud computing service providers establish a trust relationship in advance. The users only need to register and log in to a service provider that trusts each other, and then they can access all service providers without having to repeat them. It not only improves the ease of use of the cloud service, but also makes the user more convenient, and saves the independent and complex identity management of the cloud service provider.

As a window facing the outside world of the cloud system, API security controlled mechanism should be deployed to record and monitor API access to prevent malicious users from using the API to implement attacks. The digital signature technology can be used in API protection. For all calls to API, the X.509 certificate or the customer's private key signature is required, and the verification is performed on the cloud platform. Only the legitimate user who passed the authentication will be given the call permission of API.

The isolation technology between multi-tenants can be implemented at different levels of the cloud architecture. The physical layer isolation method is to configure separate physical resources for each user. Different users are assigned to different servers to avoid conflicts between data. However, this method needs high hardware cost and can support a small number of users. When the platform layer is isolated, it is required to respond to the needs of different users and feed different data to different users according to the request mapping. Different users can share one physical host, but the activities of users are limited to different virtual machine platforms in the physical host. The method requires more resources, but the hardware cost is low, and the number of supported users is more than the physical layer. Application layer isolation adopts more methods, including sandbox isolation and shared application instances. When sandbox isolation is used, each sandbox forms an application pool. The application within the pool is ensured by the isolation between the pool and the pool. The application request in the pool is handled by the background program. when the shared instance isolation mode is adopted, the application itself can support multiple users, and the isolation is implemented inside the application.

4. Analysis of experimental results

In this paper, these security technologies above are compared and analyzed in terms of security principles, attack examples, attack effects, and defense schemes. The summary is shown in Table 1.

Table 1 Comparative analysis of safety technology

kind	Safety principle	Attack instance	Attack effect	defense plan
Virtualized hardware security technology	Chip internal function module security	Malicious Firmware	Sudden crash	Identity authentication mechanism
Virtualized middleware security technology	Virtual resource pool security	Embedded attack	virtual resource pool Paralysis	Hypervisor protection technology
Virtualized software security technology	Shared memory attack	Stealing service attack	Memory read error	Virtual machine migration
Virtualized data security technology	Ownership and control of data	Security breach attack	Content tampering	Data encryption technology
Virtualized application security technology	Top-level application security	Denial of service attack	Application not available	Trusted access control technology

Through the comparative analysis of the proposed five virtualization security technologies, the corresponding security protection scheme can be obtained. The virtualized hardware device security technology can be protected by the identity authentication mechanism. When a security risk occurs, the threat is serious. The virtualized middleware security technology is mainly maintained by the Hypervisor's own protection technology. The security risks are lower than the hardware security. Virtualized software security technology can prevent memory read errors through virtual machine migration technology. Virtualized data security technology can implement content security protection through data encryption technology, and virtualized application security technology can implement the security of top layer by using trusted access technology.

5. Conclusions

The virtualization security technology in cloud computing environment is researched from five aspects in this paper. It can be seen that virtualization technology has opened the door to cloud computing. In essence, cloud computing provides us with virtualized cloud services. The maturity and wide application of virtualization technology has promoted the transformation and development of cloud computing. It can be said that virtualization technology is a key factor in the development of cloud computing. However, virtualization technology has many security risks. The security problem of virtualization technology in cloud computing is also an important issue that restricts the development of cloud computing. Only by researching and solving these problems can we continuously improve and develop cloud computing.

References

[1] Jing C, Tao Z. Concert: A Cloud-Based Architecture for Next-Generation Cellular Systems. IEEE Wireless Communications, 2014, 14, pp. 14–22.

[2] Huangke C, Xiao M. Towards Energy-Efficient Scheduling for Real-Time Tasks under Uncertain Cloud Computing Environment. The Journal of Systems and Software, 2015, pp. 20–35.

[3] Da Z, Chung N. An Energy-Saving Algorithm for Cloud Resource Managemeng Using a Kalman Fliter. International Journal of Communication Systems, 2014, 27, pp. 4078–4091.

[4] Siva T M, Lei Y. Heavy Traffic Optimal Resource Allocation Algorithms for Cloud Computing

Clustres. Performance Evaluation, 2014, 81, pp. 20–39.

[5] Zhi G, Guo S. Using Priced Timed Automaton to Analyse the Energy Consumption in Cloud Computing Environment. Cluster Computing, 2014, 17, pp. 1295–1307.

[6] Junaid S, Kashif B. Data Center Energy Efficent Resource Scheduling. Cluster Computing, 2014, 17, pp. 1265–1277.