Design of the Security Mechanism for a BPO Cloud Computing Platform

Huaihai Hui
School of Electronic and Electrical Engineering,
University of Leeds,
Leeds, LS2 9JT, United Kingdom.
h.hui@leeds.ac.cn/huihuaihai@ucas.ac.cn

Des McLernon and Ali Zaidi
School of Electronic and Electrical Engineering,
University of Leeds,
Leeds, LS2 9JT, United Kingdom.
{d.c. mclernon & s.a.zaidi}@leeds.ac.uk

Abstract - The security of a Cloud Computing Platform (CCP) is a key factor in its ability to operate successfully. Currently, the security issues of the physical resource layer and the user application layer of the cloud computing platform have been significantly studied in the field of information security and have already mature products and solutions. This research is aimed at the complex Business Process Outsourcing Cloud Computing Platform (BPO-CCP) for the banking and insurance industries. In particular we are concerned with the BPO-CCP's virtualization security, cloud data security, access control, user authentication and authorization, and cloud computing auditing. This paper analyzes the specific needs of the platform's security. Then the Security Mechanism of the BPO Cloud Computing Platform (SM-BPO-CCP) is designed. During its implementation (around five years at the time of writing) this SM-BPO-CCP that we have designed has efficiently provided security protection for up to twenty BPO companies with each having more than 1000 employees. This SM-BPO-CCP linked to ten large banks and insurance companies, none of which experienced any security issues due to the protection offered by the SM-BPO-CCP.

Keywords - Security Mechanism;Cloud Computing;BPO

I. INTRODUCTION

With the globalization of economic development, and the continuous refinement of international division of labor and cooperation, large multinational companies not only implement manufacturing outsourcing, but also implement Business Process Outsourcing (BPO) [1]. BPO means that the company outsources some repetitive non-core or core business processes to suppliers. Now with the development of advanced network technologies, high-speed data networks, and increasing bandwidth capabilities, the scope of outsourcing is expanding. Outsourcing is no longer limited to the outsourcing of a specific component but it expands the outsourcing of a range of administrative matters [2]. Currently, BPO can provide financial, insurance, medical, human resources, mortgage, credit card, asset management, customer care, and sales service.

The BPO Cloud Computing Platform (BPO-CCP) referred to in this paper mainly serves the back-office business process outsourcing of the banking and insurance industries. The types of outsourcing of these businesses include car loans, mortgages, credit cards in the banking industry, and new contracts and claims for life insurance in the insurance industry. This type of business is more complex for BPO services because it has basic management functions such as data entry or billing.

At the same time, it requires the ability to make decisions and solve problems. It is a BPO service for complex transactions. Therefore, it requires the BPO supplier's operators to have high skills and the BPO platform to have high security standards.

Most importantly, the BPO-CCP for this type of business is directly linked to the core business systems of major international banks and insurance companies. The BPO-CCP needs to accept business outsourcing tasks/data from the core system of the bank or insurance company, and then process these outsourced services on the BPO-CCP. Finally, the results/data are fed back to the core business systems of these large banks or insurance companies. In other words, this BPO-CCP has stringent requirements for security mechanisms. It must ensure the security of its own platform, and it must also ensure the security of the platform it links to. Based on the above characteristics, this paper analyzes the specific requirements of the security of the platform, and at the same time, designs and studies the Security Mechanism of the BPO Cloud Computing Platform (SM-BPO-CCP).

II. SM-BPO-CCP

Currently, the physical resource layer of the cloud computing platform includes computer clusters, distributed storage, network facilities, databases, and system software. These common security issues have been well studied in the information security field and have proven products and solutions such as firewalls, intrusion detection, and anti-virus systems [3]. The user application layer also has cloud pages to prevent tampering, user threat isolation, anti-spam and other measures to ensure security. As we all know, the security system of the cloud computing platform involves not only technical security issues, but also security issues at the regulatory and policy levels.

This paper only focuses on the security technology mechanisms of cloud computing platforms. This research is aimed at the complex business BPO cloud computing platform serving the banking and insurance industries. In particular, it looks at the BPO-CCP's virtualization security, cloud data security, access control, user authentication and authorization, and cloud computing auditing. Figure 1 shows the overall framework of SM-BPO-CCP.

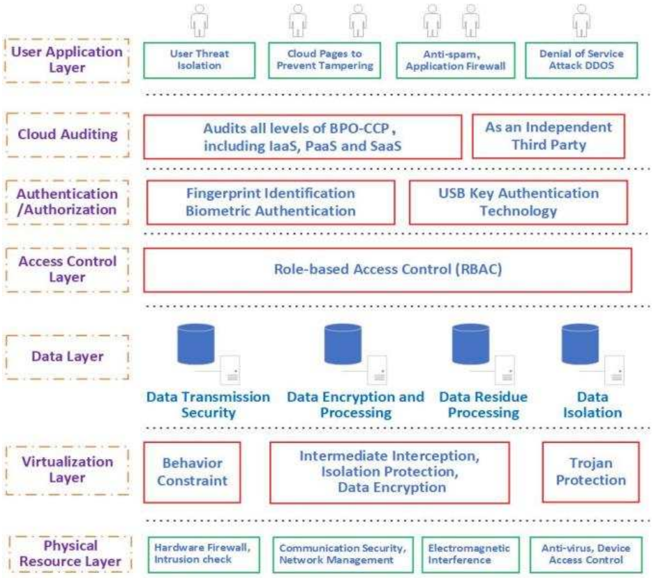
User Application Layer
User Threat Isolation
Cloud Pages to Prevent Tampering
Anti-spam, Application Firewall
Denial of Service Attack DDOS
Cloud Auditing
Audits all levels of BPO-CCP, including IaaS, PaaS and SaaS
As an Independent Third Party
Authentication /Authorization
Fingerprint Identification Biometric Authentication
USB Key Authentication Technology
Access Control Layer
Role-based Access Control (RBAC)
Data Layer
Data Transmission Security
Data Encryption and Processing
Data Residue Processing
Data Isolation
Virtualization Layer
Behavior Constraint
Intermediate Interception, Isolation Protection, Data Encryption
Trojan Protection
Physical Resource Layer
Hardware Firewall, Intrusion check
Communication Security, Network Management
Electromagnetic Interference
Anti-virus, Device Access Control

Figure 1. Framework of SM-BPO-CCP

III. VIRTUALIZATION SECURITY

Virtualization technology is the key technology to realize cloud computing [4]. Providers of cloud computing platforms that use virtual technology must provide security assurance to their customers. The virtualization layer of the BPO-CCP includes the most basic software system of the cloud platform. The virtual machine monitor is a virtualization management software running between the guest operating system and real physical hardware. It directly manages computer hardware resources and provides multiple isolated virtual execution environments for the operating system. It is at the heart of virtualization technology and is responsible for most of the work in the tedious virtualization effort. The BPO-CCP virtual machine monitor implements a series of monitoring and management of active subjects through a behavior constraint mechanism. Behavioral constraints emphasize that in a cloud computing environment, users require their service requests to be properly executed by the cloud computing platform, and the data is not maliciously modified or used. The BPO-CCP requires that both intentional and unintentional security attacks in the application requested by the user will not affect the overall platform.

The Virtualization Security System (VSS) is designed to constrain the behavior of the operating system. It can protect cloud computing services in an untrusted environment. It establishes a behavioral constraint layer that is transparent to the application and operating system. The BPO-CCP's constraint layer completely controls the interaction of data between the operating system and the application, thus preventing private resources from being maliciously stolen.

The behavior constraint layer established by the VSS is transparent and mandatory. Transparency ensures that applications can run in the system without special modifications. Mandatory means that if the operating system needs to call the platform's resources, it must pass the VSS. If a malicious operating system wants to bypass the operating system of the platform to operate on hardware resources, it will not be able to call the system because there is no corresponding permission for the hardware resources. The VSS defines user applications as two types of normal and constrained applications. Normal application users do not need to be bound by the VSS when making system calls, which can keep the system running efficiently. Constrained application users must go through the VSS when interacting with the operating system to ensure that their operations are allowed. The VSS uses three methods to complete the protection of data: Intermediate interception mechanism, isolation protection mechanism, and input/output data encryption mechanism.

A. Intermediate Interception Mechanism

- The control handoff between all processes by the VSS and the kernel of the operating system must be constrained by the behavior of the VSS.
- Data interaction between all processes to the VSS and the kernel of the operating system must be constrained by the behavior of the VSS.
- An untrusted operating system must be authorized by the VSS when it invokes certain privileged physical resources.

In general, the interaction between the user's application and the operating system is done through system calls. In the traditional computing mode, the user application interacts with the operating system immediately through a system call. In the VSS, the user's application process must be monitored by the trusted system management layer in the virtual machine monitor before the system can be called.

B. Isolation Protection Mechanism

- The VSS's isolation of the process's context is done by hiding registers that are not used in system calls. The VSS has three parts for memory isolation: application mapping hiding for page table management; tracking page swapping in/out to prevent unauthorized access; and troubleshooting for memory swapping in/out.
- When the VSS intercepts a system call from a constrained process, it saves the context of the process and provides only the necessary information. The process's context is restored when the process returns from the operating system.
- The VSS page table hides the information that the page table of the constrained process has saved before entering the operating system. Then, the page table containing the mapping information is given to the operating system. Finally, the page table is loaded into memory when the result of the process call is returned to the user process.

C. Data Encryption Mechanism

Data protection technology is used to protect the privacy of user data to ensure that it is not maliciously modified or used [5]. The VSS protects user data by encrypting I/O data.

- Because public files are accessed by many processes to support the operation of the system, so public files do not need to be encrypted. In the VSS, a list is specifically set up to record public files such as system configurations to indicate that these files do not need to be encrypted. When some processes contain data or private files that require privacy protection, the VSS will indicate that this type of data needs to be encrypted.

- Firstly, the VSS encrypts the contents of the file using a symmetric key. Secondly, the VSS re-encrypts the symmetric key along with the assigned platform label through the public key of the target platform. Finally, the VSS places the encrypted content at the end of the encrypted file. The advantage of this encryption method is that the VSS does not need to know the file format of the encrypted file and can also perform encryption operations.
- In addition, the BPO-CCP also adds a virus Trojan protection engine to the virtualization layer. In this way, the bottom layer can be protected from viruses and Trojans, thus ensuring the security of the base layer of the cloud platform.

IV. Cloud Data Security

Since the data on the BPO-CCP eventually runs on the distributed computing nodes, so if a distributed computing node is compromised, the user data in the memory of the compromised node will be completely exposed. The BPO-CCP needs to be encrypted before the computing task is assigned. And when the data of the distributed computing node returns, the BPO-CCP also has a corresponding verification method to ensure that the data has not been tampered with.

A. Data Transmission Security

Data transmission on the public network can be easily intercepted, so the information transmitted to the cloud computing platform needs to be encrypted to avoid plain text in the transmission process. The transmission protocol used to transmit data over the Internet must also ensure data integrity. Although the use of encrypted data and the use of non-secure transport protocols can also achieve confidentiality, the integrity of the data cannot be guaranteed. In addition, the BPO-CCP is able to prevent detection and prevent external information from being received. The BPO-CCP is immune to radiation and prevents useful information from being radiated in a variety of ways. At the same time, the BPO-CCP uses physical measures such as restriction, isolation, masking, and control to protect data from being leaked.

B. Data Encryption and Processing

The BPO-CCP uses cryptographic techniques to encrypt data. After the data is encrypted, the ciphertext retrieval and processing problem must also be resolved. Because data loses many features when it becomes ciphertext, it can cause many data analysis methods to be unusable. The BPO-CCP ciphertext retrieval uses two methods: a secure index-based method is used to retrieve the index query keywords by establishing a security index for ciphertext keywords. A ciphertext scanning method is also used to compare each word in the ciphertext, which confirms whether the keyword exists and counts the number of occurrences.

C. Data Residue Processing

Data retention is the physical behavior of data that remains after being erased in some form. After the storage medium is erased, some physical characteristics may be left to enable the data to be reconstructed. In a cloud computing environment, data retention is more likely to inadvertently reveal sensitive information [6]. Therefore, the BPO-CCP needs to be completely cleared before the storage space in which the user's private information resides is released or reassigned to other cloud users, whether the information is stored on the hard disk or in memory. The storage space of resources such as files, directories, and database records in the BPO-CCP system needs to be completely cleared before being released or reassigned to other cloud users.

D. Data Isolation

The greater the number of customers for the BPO-CCP services, the higher the data isolation and security requirements. The BPO-CCP uses a mature architecture to help the system achieve data isolation: shared schema multi-tenancy and separated database architecture.

Shared schema multi-tenancy: All software system clients share the same database instance and the same database table but it can distinguish the affiliation of the data through a Tenant ID field. Shared schema multi-tenancy maximizes the storage power of a single database, and the hardware cost is very low. But it adds extra complexity to the program developer. Since the data of multiple customers coexists in the same database table, additional business logic is needed to isolate the data of each customer. In addition, the cost of implementing disaster recovery for this architecture is also very high. This is because it not only needs to write code to achieve data backup, but also it needs to delete and insert a large number of database tables when restoring data.

Separate database architecture: Each software system customer has its own database. Because each customer has a separate database, this architecture makes data security and disaster backup very efficient and convenient. But its hardware costs are very high.

V. Access Control

Access control ensures that authorized users can obtain access to the required resources while denying access to unauthorized users. It restricts the access rights of access subjects (users, processes, services, etc.) to access objects (data, files, systems, etc.), thereby allowing the computer system to be used within the legal scope. It grants permissions to users who are recognized by the system, restricting or denying unauthorized access. Access control has several types, such as autonomous access control model, mandatory access control model, and role-based access control (RBAC) [7] model.

The BPO-CCP uses a RBAC model. It assigns roles to subjects in the system to implement access control. The user obtains a certain role after being authenticated, and the role is assigned certain permissions. The user accesses system resources in a specific role, the access control mechanism checks the permissions of the role and decides whether to allow access. At the same time, users are not accessing the system with the same registration status and permissions from start to finish. Its advantages are separation of responsibility, role stratification, role activation, and constraints on user role relationships.

The process of BPO-CCP users accessing the information system is actually the process of the subject (cloud user) accessing the object (cloud information system). RBAC functionally defines roles through the combination of permissions, and logically separates subjects and objects through roles. RBAC associates users with roles and associates roles with questioning permissions. RBAC makes access control more flexible and easier to manage.

VI. User Authentication and Authorization

The BPO-CCP runs the identification and authentication of the user. Identification refers to the identity of the user to ensure that the user is identifiable and unique in the system. The authentication system authenticates the user's identity.

The BPO-CCP adopts fingerprint identification biometric authentication and USB Key combination authentication technology. Fingerprint recognition biometric authentication technology is the most reliable method of identity authentication because it directly uses the physical characteristics of people to represent the digital identity of each individual. The possibility that different people have the same biological characteristics is negligible, so it is almost impossible to be counterfeited.

The USB Key authentication technology adopts a strong two-factor authentication mode of one key at a time combined with software and hardware. It solves the relationship between security and ease of use. The USB Key is a USB interface hardware device that has a built-in smart card chip to store the user's key or digital certificate. It uses the cryptographic algorithm built into the USB Key to authenticate the user. At the same time, the USB Key has the advantages of being safe and reliable, convenient to carry, convenient to use, and low in cost. The authentication method of storing digital certificates using the USB Key has become the main authentication mode at present.

VII. Cloud Computing Auditing

Auditing is an important tool to support the safe operation of the BPO-CCP, which accurately reflects security-related events in the operation of the system. Audits permeate every process of the BPO-CCP, including operating system, databases, and network equipment, etc. It audits all levels of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

The cloud auditing system accesses data in the cloud computing platform as an independent third party. It provides a comprehensive record and audit of the BPO-CCP's own situation.

The cloud auditing system records all data access behaviors independently, and the automatically generated audit reports can discover the data being accessed and used. It records the trajectory of the data store and provides a data storage analysis report. It comprehensively monitors the storage status of cloud data, tracks data movements, and identifies potential data conflict risks. It monitors the availability of data on the cloud platform in real time. It records the process of changing important data. A security alert is sent when it finds an abnormal condition, which reduces data loss.

VIII. Mechanism Effect

The data processed by the BPO-CCP, whether it is a mortgage or a car loan, is the financial data of the company or individual. At the same time, this data is related because of the needs of business processing. For example, if you want to evaluate a customer's credit rating, you need to correlate all the financial data related to it. So, the data processed on the BPO-CCP is almost all about the financial data of a company or individual. The security requirements for such data processing are very high. During its implementation (around five years at the time of writing) this SM-BPO-CCP that we have designed has efficiently provided security protection for up to twenty BPO companies with each having more than 1000 employees. This SM-BPO-CCP linked to ten large banks and insurance companies, none of which experienced any security issues due to the protection offered by the SM-BPO-CCP.

References

[1] Mary C. Lacity, Leslie P. Willcocks, (2008) "Global outsourcing of back office services: lessons, trends, and enduring challenges", Strategic Outsourcing: An International Journal, Vol. 1 Issue: 1, pp.13-34.

[2] Gyeung- Min Kim, (2008) "E- business strategy in Western Europe: offshore BPO model perspective", Business Process Management Journal, Vol. 14 Issue: 6, pp.813-828.

[3] Shancang Li, Theo Tryfonas, Honglei Li, (2016) "The Internet of Things: a security point of view", Internet Research, Vol. 26 Issue: 2, pp.337-359.

[4] Christinger Tomer, (2017) "Cloud computing and virtual machines in LIS education: options and resources", Digital Library Perspectives, Vol. 33 Issue: 1, pp.14-39.

[5] Julio Angulo, Simone Fischer- Hübner, Erik Wästlund, (2012) "Towards usable privacy policy display and management", Information Management & Computer Security, Vol. 20 Issue: 1, pp.4-17.

[6] Marc Walterbusch, Adrian Fietz, Frank Teuteberg, (2017) "Missing cloud security awareness: investigating risk exposure in shadow IT", Journal of Enterprise Information Management, Vol. 30 Issue: 4, pp.644-665

[7] Tran Khanh Dang, Tuyen Thi Kim Le, (2014) "Towards a flexible framework to support a generalized extension of XACML for spatio-temporal RBAC model with reasoning ability", International Journal of Web Information Systems, Vol. 10 Issue: 2, pp.131-150.