2014

ISSN : 0974 - 7435 Volume 10 Issue 21

BioTechnology

An Indian Journal

FULL PAPER

BTAIJ, 10(21), 2014 [13062-13066]

Study of data access control method based on cloud computing

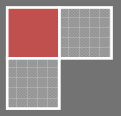
Sun Rui Wang Xiaoyan
Henan Vocational and Technical College, Zhengzhou, 450046, (CHINA)

ABSTRACT

In the public cloud computing environment, users can not control the storage position of the data effectively, so it can not guarantee the security of user' data and there is a big security risk. In order to ensure the security of user' core data in cloud computing, this study proposes the idea of hybrid cloud architecture in terms of protecting the security of user' data and designs a user' core data protection model based on cloud computing. It decomposes the data on the basis algorithm and the data after decomposition are the core data and general data. When the general data is handled by the gateway filtering, the data which is blocked is stored in the private cloud and the data which is not blocked is stored in the public cloud; when storing the core data, the security and privacy of these data should be protected. These data is stored in the private cloud or stored in the public cloud with encryption. Although there are many studies on the application of cloud computing, it is still in the development stage and the problem related to data security has not been solved effectively. And from the perspective of cloud computing users, this problem needs a long-term concern. The security of the core data can be effectively protected after processing. This study designs data classification algorithm and selects of existing mature network products to build out the core data protection system of enterprises based on cloud computing. And the system is applied to an enterprise for one-year experiment to verify the validity of the model. This study is expected to explore new ways to protect the user' core data based on cloud computing.

KEYWORDS

Cloud computing; Core data; Security model; Protection system.



INTRODUCTION

Cloud computing is an emerging computing model and the model is based on the Internet[1]. As a new service model, its architecture model is shown in Figure 1. Through the front-end interaction interface and to find the service catalog, the user selects the required service and send service requests to the management system, then the system verifies and finds the resources, and then call for the deployement tool to complete the excavation of the resources in cloud. In this model, the user can not only enjoys the high-performance computing, but also carries out the high-capacity storage of user' data. And, while saving the high equipment cost, it avoids the transport and maintenance costs of equipment at the same tine[2]. Based on their convenience and scalability, the use of cloud computing can remove the management and maintenance of IT infrastructure, allowing the user, especially the user of medium and small-sized enterprises to focus more on the development of their core business. Because of the advantages of cloud computing, it is becoming the cynosure of more and more eyes of the users, especially the eyes of the enterprises.

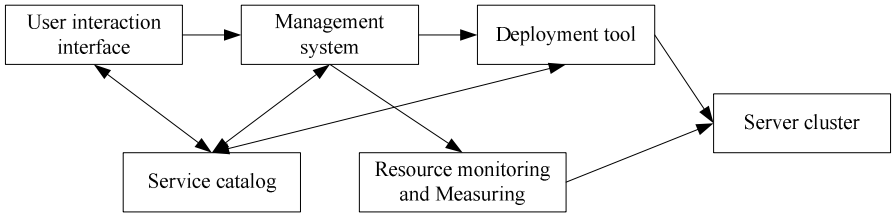


Figure 1 : The architecture schematic diagram of cloud computing

In general, cloud computing resources are not the localization, which means that if the user chooses the cloud computing, the data that the user uploads for cloud computing will be stored in different databases randomly. These databases are offered by the cloud computing service provider. When storing the data, it would make several backups to avoid the loss of data. For the user, it exist the safety problems of data transmission and storage[3]. How to protect the user's core data, regardless for the user, or the cloud computing service provider, it is the important problem that may restrict the promotion and development of cloud computing.

With the rapid development and popularity of data informatization as well as the characters of convenience, practical and low cost of cloud computing, more and more enterprises user consider to build their own business system in cloud computing environment. The main problem they concerned is the security of data in cloud computing. In the long-term informatization construction process, it is easy to find that most of the data of user can be divided into two categories, namely, general data and core data. The general data also is called the external data, which can be understood as part of the user data can be disclosed to the public on the literal meaning. The importance level of these data is low and the loss of them could not lead to the lost of user, so usually these data can be stored out of the controllable range of user, which means that there is no problem even if these data are stored in the public network disk. However, the core data is internal data, which usually contains the user's important information, such as critical business processes or customer data and other information. These data reflect the core competitiveness of the user. So from the user's point of view, the security these data is very critical. They want to store such data in their own controllable range, such as stored in local[4].

According to the user requirement to protect the core data security, combined with the characteristic of data storage and backups randomly in the cloud computing environment, the enterprises users expect to design a hybrid cloud structure that meets the basic needs of users to protect the security of core data. This study analyzes the different needs of users for the data, including the core data and general data. Then, it designs the user core data protection model on the basis of cloud computing and applies the model into the actual business of an enterprise to do experiment to verify the practicality and effectiveness of the model. After the actual operation in the enterprise, it can prove that the user core data protection model built in this study has good practical results in the protection of user core data, which basically meets the design requirements of the model as well opened up a viable path for future research[5].

MODEL DESIGN

The user core data protection model is carried out based on the deployment scheme of cloud computing, so the choice of cloud deployment scheme determines the display of the function of core data protection model[6]. In accordance with NIST, cloud computing deployments can be divided into four categories, namely, public cloud, private cloud, community cloud and hybrid cloud. Whether in terms of the transmission security of data or the storage of data, the deployment schemes of these four cloud computing have their own characteristics. Combined with the needs of the above model, this study mainly analyzes the security and usability.

Generally, the public cloud is rented from the cloud computing service provider by user in accordance with his or her needs. The cloud computing service provider builds the servers at first and then they are selected by the user. From the user's point of view, the performance of public cloud is better and the cost is lower. But, due to the user's data is stored in the service provider's cloud computing environment randomly, so the disadvantage of the public cloud is the security problem of user data, which is the obstacle for the development of public cloud.

There are two ways for the private cloud. One is the service provider provides the construction to the user, but the service of this part is independent after the rent of user; the other is formed by the construction of the interior of user organization[7]. The private cloud not only has the advantages of high performance and flexibility of cloud computing, but also can solve the data security problem of public cloud. In the four cloud deployment scheme, the data security is the highest in private cloud. But the private cloud also has its disadvantages. Whether the cost of construction or the cost of operation and maintenance, the spending of private cloud is high and the general medium and small-sized enterprises can not afford it. So because of financial problem, the development of private cloud is influenced.

Community cloud likes the community in the usual sense. It is constructed by a group of enterprises or organizations and these organizations or enterprises have common interests. After the completion of construction, the community cloud environment is use by all the members together, and the data and applications are shared among them. So in this architecture of cloud computing, it is not appropriate to store the core data and there is no confidentiality among the internal members.

Hybrid cloud is composed by two cloud environments. Generally, the two cloud environments refer to the public cloud environment and private cloud environment. In which, the public cloud carries out the storage of general data and the private cloud is responsible for the storage of user's core data storage, includes the storage of user's core business computing. In this deployment, the unnecessary general data or the noncritical part in business computing can be completed by the rent form of public cloud, which can save the costs; The critical core data or the core technology can be stored by an independent private cloud architecture platform. When storing the user data, the hybrid cloud not only takes into account of the advantages and disadvantages of the public and private cloud comprehensively, but also saves time and money for user. So, usually, some enterprise customers who require the higher data security would choose this kind of cloud computing scheme. The structure diagram is shown in Figure 2.

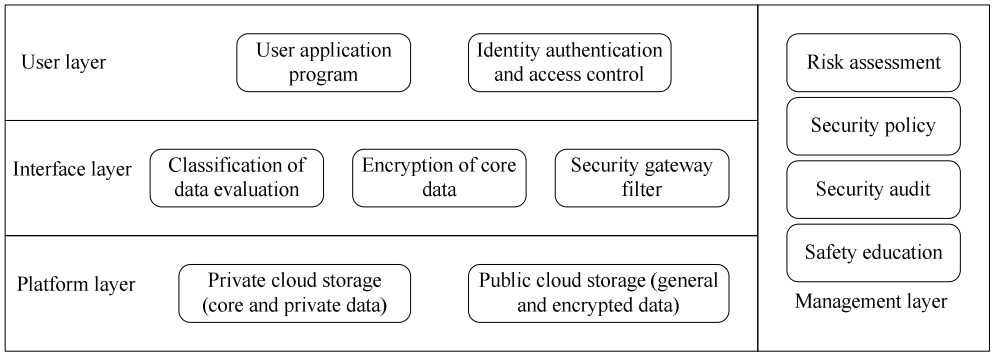


Figure 2 : The protection model of user core data based on cloud computing

From the Figure 2, it can be seen clearly that the protection of the model is divided into four layers, namely the platform layer, the interface layer, the user layer and the management layer. For this model, the basic task is to store the data and the task is completed in the platform layer. The platform layer comprises two parts: public cloud storage and private cloud storage. After assessment, the model carries out the processing of gateway filtering for the general data, the data which is blocked is stored in the private cloud and the data which is not blocked is stored in the public cloud; when storing the core data, the security and privacy of these data should be protected. These data is stored in the private cloud or stored in the public cloud with encryption. So from this point of view, this model is implemented on the architecture of hybrid clouds. So, if the normal user wants to achieve the effect of data security and they have enough security protection, they can meet the requirement of security protection similarly.

The task of interface layer is to classify and encrypt the data. According to the demand of the model, the interface layer uses the data assessment and classification algorithm to help the user to control the core data. Usually, the equipment and procedures of interface layer are arranged in the inlet and outlet of private cloud. This work is very crucial for the design of the model, which can affect the protective effect of the data directly.

There are two tasks for the user layer, which are to authenticate the user's identity and to provide application data to cloud computing environment through login authentication. This layer can ensure the identity of user in order to protect the security of the data in cloud computing platform. The management layer is the guarantee of the operation of all the work and it supports the realization of the entire model. Compared with the traditional network environment, the security mechanism of cloud computing has no difference, but there are security risks which can not be solved by technology. However, the auxiliary management methods can solve these problems. The formulation and implementation of safety management strategies can realize the purposes to protect the core data.

EXAMPLE FOR VERIFICATION

According to the needs of user, applying the model to the information construction of an enterprise, this study design a “enterprise core data protection system based on cloud computing ". The design logic structure diagram is shown in Figure 3. Figure 4 shows a schematic diagram of the network topology. Through the one-year actual operation, the designed system can achieve the purpose to protect the user core data.

When building the private cloud environment, the software and hardware resources of enterprises are used in basis of the principle of conservation. These resources include 4 blade server, a set of storage array, a three-tier core switch, a gateway and a virtualization platform. The construction of virtualization platform is on the basis of software and hardware. Then the simulation of the platform environment has taken place on the platform. And finally it installs the application required by the enterprises to realize the full function of private cloud.

When selecting the public cloud environment, in order to achieve the purpose of transmitting and obtaining the stable data while save money at the same time, by comparing, the free cloud storage is chose finally. The advantage of the platform is that there is a convenient program development interface. But there are disadvantages, such as the slow speed of network transmission. General speaking, it can meet the need.

When building the protection system, the key part is the construction of interface layer. It not only has the relative subjective tasks such as quantitative criteria, but also needs to meet the corresponding functional requirements in the hardware products to filter the security gateway. After the research and experiment on the requirement, the "evaluation of data importance" algorithm is introduced in the problems of data evaluation and classification.

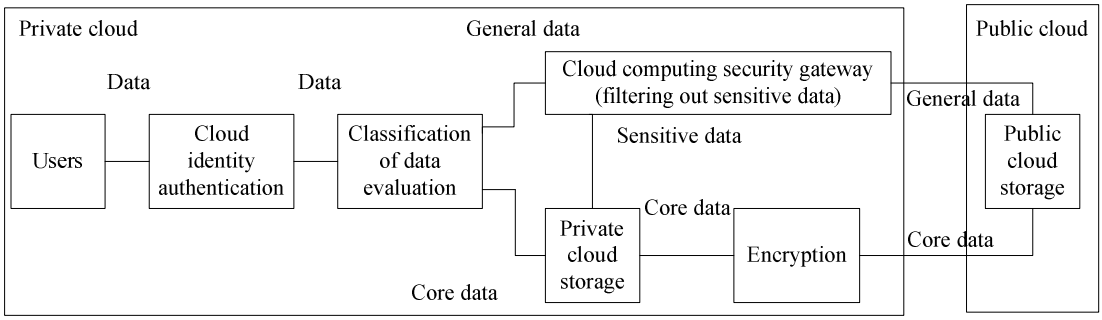


Figure 3 : The core data protection system enterprise

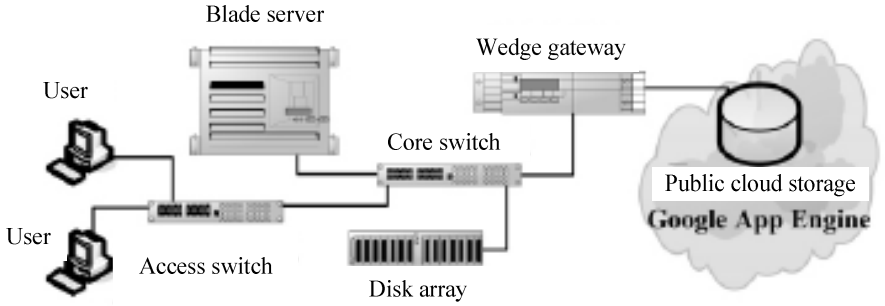


Figure 4 : The network topology of data protection system

Algorithm description

The algorithm which is introduced mainly evaluates the importance of the data in two aspects: the evaluation to the data value and the evaluation to protection strength that the data needed. The judge criterion of the former is that if such data is revealed, how mach loss it will cause for the enterprises; the evaluation to the latter is the confidential strength of such data in accordance with the requirement of enterprise. According to the judge criterion, the algorithm marks the score for application data and classifies the data according to data value, and finally to the process data. When classifying the data, the algorithm composes a user evaluation team. All members of the team assess the leaders of various departments and the core technical staff and the security staff to make the scoring standards to show the importance of assessing and quantifying data. TABLE 1 shows the classification of data importance. From the table, the diagonal of the table is the data after evaluation and it is not necessary to distinguish their grades. The following data is the core data and the safety and privacy of the data should be protected. Also, this data should be stored in the private cloud or in the public cloud with encryption; the above data is general data and these data should be processed by the gateway filtering. The data which is blocked is stored in the private cloud and the data which is not blocked is stored in the public cloud. After this algorithm, the core data can be protected effectively.

Identity authentication and security gateway

The designed system adopts the identity authentication device to ensure the validity of identity authentication. The identity authentication device is designed based on strong security considerations. And the certified product which is selected comes from the RSA Company which can provide strong identity authentication to the enterprise to prevent online fraud risk. It also can provide the anti-fraud solutions by providing end to end protection. By the verification, enterprise has recognized the performance of the product. The relationship among each entity is shown in Figure 5.

TABLE 1 : The classification of data importance

Value level	Protection strength			
	Advanced	Intermediate	Primary	Zero level
The first class		General data	General data	General data
The second class	Core data		General data	General data
The third class	Core data	Core data		General data
The fourth class	Core data	Core data	Core data	

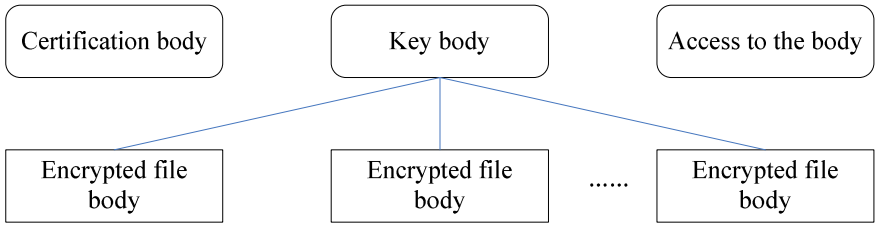


Figure 5 : The relationship among certification body, key body and file body

There are no mature security gateway products for cloud computing in the market. So, during the selection of the gateway, the products with comprehensive function are the main selection targets and finally the "BeSecure Web" security gateway is chose. The product is from the Wedge Network Company and it is designed for Web2.0. Also, it is applicable in the private cloud environment and shows a strong protective function. It not only can detect and prevent the spread of malicious software, but also can prevent the loss of data. Its ultimate function is to carry out the complete safety testing for the deep content.

Already mentioned above, the core data can be encrypted and stored in the public cloud. In this system, it develops the encryption and decryption interface programs to carry out the core data processing to achieve the storage operations of public cloud. The practical algorithm is AES-128 algorithm, and it ultimately ensures the security of core data.

CONCLUSIONS

Although there are many studies on the application of cloud computing, it is still in the development stage and the problem related to data security has not been solved effectively. And from the perspective of cloud computing users, this problem needs a long-term concern. In data security protection of cloud computing, the design of the data privacy is wider. This study selects the core data protection problem to make the application research in the enterprise customers. Relatively speaking, the enterprise customers' requirements are higher for the privacy and security of data and the user group is much larger. So from the perspective of such users, the construction of the core data protection model based on cloud computing has its practical significance. In this study, the user's data is based on data evaluation and classification algorithm which is divided into core data and general data. The private and sensitive data are stored in the private cloud or the public cloud with encryption so as to guarantee the security the user data in the greatest degree. In the system, in order to realize the security function, although it uses some existing mature products, the system still not perfect from the point of the actual practice and the relevant studies are still needed.

REFERENCE

[1] Feng Dengguo, Zhang Min, Zhang Yan; Study on cloud computing security [J], Journal of Software, **22(1)**, 71-83 **(2011)**.

[2] Wang Liwei; Intelligent identity authentication protocol based on cloud computing, [J], Computer Science, (monograph), **37(8)**, 45-48 **(2010)**.

[3] Shen Lijun; Research of cloud storage and its security [J], Computer Knowledge and Technology, **7(16)**, 3829－3832 **(2011)**.

[4] Hung Yongfeng, Zhang Jiuling, Li Xing; Encrypted storage and its retrieval in cloud storage applications [J], ZTE Technology Journal, **16(4)**, 3-35 **(2010)**.

[5] Liu Fan, Yang Ming; Ciphertext policy attribute based encryption scheme for cloud storage, [J], Application Research of Computers, **29(4)**, 1452－1456 **(2012)**.

[6] Lu Zhiquan, Zhang Min, Feng Dengguo; Cryptographic access control scheme for cloud storage, [J], Journal of Frontiers of Computer Science & Technology, **5(9)**, 835－844 **(2011)**.

[7] Sun Guozi, Dong Yu, Li Yun; CP-ABE based data access control for cloud storage, [J], Journal on Communications, **32(7)**, 146-152 **(2011)**.