Journal of Applied Science and Engineering Innovation, Vol.3 No.5, 2016, pp.185-188
ISSN (Print): 2331-9062
ISSN (Online): 2331-9070

Resources Sharing Patterns Based on Cloud Computing

Hui Li[1], Hong-Yan Liu[1],Xu-Gang Liu[1], Xiao-ting Li[1], Le Zhao[1]
[1] *Xi'an communication college, Xi'an 710106, China*

Abstract: By analyzing the security of information resources sharing in cloud computing environment, we put forward the detailed introduction of the constitution and function of cloud information resource flow architecture. Therefore, the problems of network source information management, supervisory control, exploitation and utilization can be solved.
Keywords: emergency communication network; Ad hoc network; wireless sensor network; WiMAX

INTRODUCTION

With the development of cloud computing, security issues have become increasingly prominent, becoming an important factor restricting the development of cloud computing. More and more companies hold a skeptical attitude towards cloud computing because of security issues. According to IDC reports, there are more than 74% of users believe that security issues are the main problem limiting the development of cloud computing.

Cloud computing is the development of concurrent computation, distributed computation and grid computing, as well as the evolution of the virtualization, utility computing, infrastructure as a service (LaaS), platform as a Service (PaaS) and software as a service (SaaS) [1]. The cloud computing based development and utilization of information resources can mix together with the service idea, and change the conventional pattern of information resources collecting via the advantages of large-scale sharing using cloud computing. What's more, it can mine the potential link among different information, improving the utility value of information. The development and utilization of information resources usually depends on data centre, which is the centre with integrated data, business system development and deployment, various services as well as comprehensive safety protection, rather than the past one - the traditional and isolated data centre.

CLOUD COMPUTING

- **Concept of cloud computing**

The concept of cloud computing was defined by IEEE International Conference on Web Services (ICWS), in Beijing, 2008. This definition consists of three layers, which are shown as Figure 1[2]:

(1) The top layer of Figure 1 is the program layer, proving users with services by SaaS. This layer caters to users, meaning that the cloud computing is the information technology as a service (ITaaS) for users. It can offer the extensive and plastic computing as well as the application program as what the users need by the concentrated data centre.

(2) The middle layer of Figure 1 is platform layer, providing the running environments of application program or PaaS. This layer caters to the programmer and web application developers. Cloud computing is a internet-scale software development platform and running environment of them.

(3) The bottom layer is the layer of infrastructure, which is a flexible infrastructure that can offer services by distributed data centre from internet. This layer caters to the infrastructure providers and managers, who see the cloud computing as the data centre infrastructure of IP internet connection.

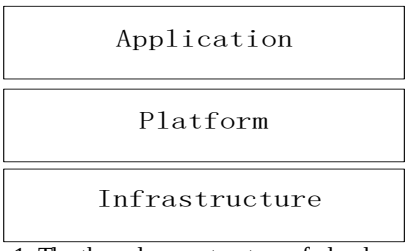

Figure 1. The three-layers structure of cloud computing.

- **Characteristics of cloud computing**

Compared to the conventional computing patterns, cloud computing has several characteristics, which are shown as follows[3]:

(1) Integration of multiple technologies: cloud computing was developed by mixing with various technologies together. Cloud computing consider the distribution of servers, PCs, mobile phones, software resources with internet, hardware resources and application services as the computing resources. Because of the dynamics, scalability, extendibility and the availability to virtualization, academic circle and IT community call it "cloud" [4].

(2) Information security: advertisements from cloud computing facilitators indicate that cloud computing can provide professional managing teams with data centre. Therefore, it's not necessary for users to worry about the safety and privacy.

(3) Convenience: users can acquire the application services with only a browser terminal equipment under the circumstance of cloud computing, without high configuration computers or facilities.

FLOW STRUCTURE MODEL OF CLOUD INFORMATION RESOURCES

Flow structure model of cloud information resources has a powerful processing ability to improve the development and utilization of network information resources dramatically [5]. The bottom layer is the physical information resources layer, which can accomplish the acquiring of original data as well as providing the hardware and visualization, which include the network equipments and storage devices; the second layer is the cloud resources management layer, providing the logical control for the sake of offering the development, running, management and control environment; the top layer is the cloud resources services layer, providing the self-service portal and application platform etc (Figure 2)[6].

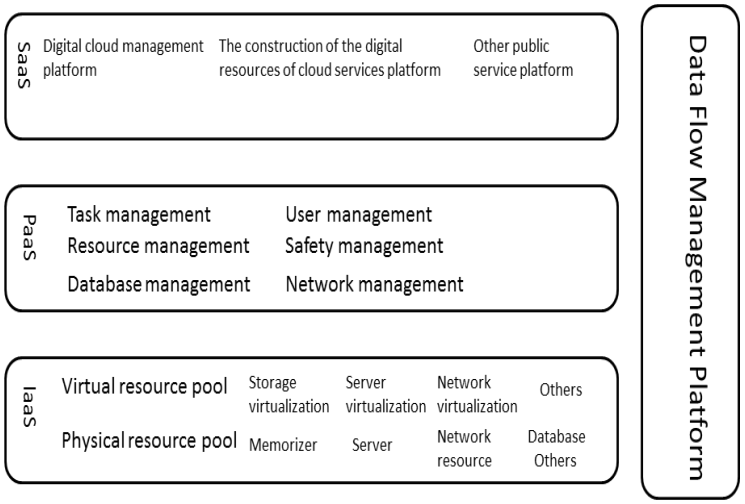

Figure 2. Flow structure model of cloud information resources.

The systematic structure model consists of three levels: the first level is the service request and operation; the second level is the ground structure and application services; the third level is the setup, accomplishment and control of the services. Among which, the core part is the second level, and it can be divided into three levels in accordance with the three types of cloud computing - LaaS, PaaS and SaaS. Thereinto, the physical resources of the lowest level involves the network resources, server resources, database resources and software resources. Virtual resources consists of different technology with the same type of constitution. The chief duty of information resources platform middleware is to manage the cloud computing resources, and provide the safe services for the upper layer by optimizing and dispatching the management loading. The management service based on rent technology can meet every users' demands to SaaS software respectively by putting the relevant cloud computing ability into the standardized WebService.

THE ISSUE OF INFORMATION RESOURCES SHARING SECURITY IN CLOUD COMPUTING

The Gartner company in US believes that cloud computing is mainly confronted with the following seven security issues:

(1)Risks of privileged user access. Privileged user management data is likely to bypass the regulation of internal procedures for control, thereby causing security risks to sensitive data from the outside of the enterprise;

(2)Compliance risks. Due to the data is submitted to the service provider for supervision, if it refuses to accept supervision and audit, it is the customers themselves who must be responsible for the security and integrity of the data;

(3)Uncertain data storage location. Because of the virtualization technology and distributed storage, the location of managed data in unclear. And cloud providers may also pose a threat to the data security;

(4)Data separation risks. Given that multi-users' data is stored in a shared cloud environment, precise data isolation should be assured. Encryption is an effective method, but it is likely to have an impact on the availability of the data;

(5)Data recovery. When a disaster occurs, whether the provider of the data and services will recover the data also affects the security of the data;

(6)Survey support risk. Because the users' log files and data may be stored together, also may be scattered in a constantly changing host and data center, so is unlikely to legally investigate the cloud computing environment;

(7)Risk of long-term availability. When the service provider is acquired, it is also important to ensure that the restored data is still available.

PREVENTION AND SOLUTION FROM A TECHNICAL POINT OF VIEW

- **Physical security**

Physical security is to protect the computer network equipment, facilities and other media from earthquakes, floods, fires and other environmental accidents and artificial operation errors and a variety of destroy caused by computer crime. It mainly includes 5 aspects: environmental safety, equipment safety, media safety. To ensure the physical security of computer information system is the premise of the whole computer information system security.

- **Access controlling technology**

With the help of improved access controlling technology, a firewall (including packet filtering and application proxy) is set up between the internal network and external network, which have already been isolated, to prevent the external network users access the internal network resources illegally and protect the special network interconnection devices in the internal network environment. It implements the inspection on the transmission of data packet between two or more networks, to determine if communication between the networks is allowed, monitor the running state of the network and achieve internal and external network isolation. At the same time, access control is achieved with the "write upward and read downward" mandatory access control technology to protect the safety of internal network, which is one of the most important and the most effective and the most economic measures.

- **Cryptography**

Cryptography is one of the most important methods in protecting information security. It is a combination of mathematics, computer science, electronics and communication of many sciences in a body of interdisciplinary. It not only has to ensure confidentiality of information encryption function, but also has a digital signature, authentication and secret saving, system security function and so on. Therefore, not only the confidentiality of information, but also the integrity and authenticity of information can be guaranteed to prevent tampering, forgery and counterfeiting. From the aspect of cryptography, there are symmetric key cryptography and asymmetric key cryptography. There is also a public key system proposed by W.Diffie and M.Hellman.

- **Virtual private network technology**

Virtual Private Network (VPN) is a technology developed rapidly in recent years with the development of the Internet. More and more modern enterprises use the Internet resources to promote sales, sales, after-sales service, and even training, cooperation and other activities. Many companies tend to use the Internet to replace their private data networks. The logic network which uses the Internet to transmit private information is called virtual private network. At present, VPN mainly uses four technologies to ensure the security, these four technologies are tunnel technology, encryption and decryption technology, key management technology, and authentication technology.

- **Safety isolation technology**

Network security threats and risks are mainly in three aspects: the physical layer, protocol layer and application layer. Maliciously cut off or communication interruption caused by high voltage belong to physical layer threat; fake network address, teardrop fragmentation attacks, SYN Flood, belong to the protocol layer threat; Illegal URL, malicious page codes, mail virus belong to the application layer attacks. From the point of view of security risks, attacks from the physical layer are rare, attacks from network layer are often, while attacks from application layer are common, which are difficult to prevent because the complexity and diversity. In the face of the constant emergence of new network attacks and the special needs of high security network, the new security concept "security isolation technology" was brought up. Under the premise of ensuring that the harmful attacks are isolated from the trusted network and that the internal information of the trusted network is not compromised, its goal is to exchange information among networks safely.

- **SSL protocol and SET protocol**

These two protocols are mainly used in the process of e-payment. SSL protocol (secure sockets layer protocol) can improve the security of data transmission between applications. Therefore, it is mainly to provide the authentication between the user and the server. The transmission security is ensured by encrypting the data. ETS protocol, the secure electronic transaction protocol, is a protocol based on information flow, which is used to ensure the security of the bank card payment transaction on the public network. It is a trusted third party certification center which reflects the various relationships of the parties to the card transaction.

- **Security audit**

In a cloud computing environment, both the user's data and computation are out of control. Therefore, it is necessary to audit the behavior of users and providers, to ensure the correct implementation of security policies, and to maintain the organization compliance. Literature Ryan KL Ko et al. proposed Trust Cloud framework, based on the method and technology to solve the problem of security audit in cloud computing environment. Audit Cloud project aims to provide basic support for ensuring the credibility and transparency of private and public cloud. Chen and Wang et al. studied on the auditing of the cloud computing, and put forward a CSIRO prototype system, which is an audit of the services deployed in the cloud computing environment.

CONCLUSION

This paper tentatively puts forward ideas on the development of network information resources development, showing that the cloud computing in the network information resources development and utilization is effective and feasible. The flow structure model of cloud information resources is a form of net information resources development and utilization, which solves the problems that net information resources management monitor and development. At the same time, its development and improvement can bring people more convenient and efficient information services in the future.

ACKNOWLEDGMENT

This work is supported by the National Science Foundation of China(61179002), Shaanxi Natural Sciences Foundation(2011JM8030).

REFERENCES

Chen Z D, Kung H T, Vlah D. Ad Hoc Relay Wireless Net2 works over Moving Vehicles on Highways. ACM Special Interest Group on Mobility of Systems, Users, Data and Com2 puting . California,USA: ACM Press ,2001. 247 - 250.

Chung Weiho, Probabilistic analysis of routes on mobile ad hoc networks, IEEE. Communications Letters. 8 (2004)8 506-508.

Dai Y X, Lian Y F, Wang H. System Security and IntrusionDetection[M]. Beijing: Tsinghua Publishing Company, 2002.

J. Liu, X.B. An, C.S. Li, Principle and Application of Wireless Network Communication, Beijing, China, 2002.

Kachirski O, Guha R. Intrusion Detection Using Mobile Agents inWireless Ad Hoc Networks[C]. IEEE, July 2002:10-12.

Ljubica B, Levente B, Srdjan C, et al, Self-organization in mo2bile Ad hoc network : the approach of terminodes, IEEE Communication Magazine. 39 (2001)6 166-174.

Macker J ,Corson S. Mobile Ad Hoc Networks (MANET)[EB/OL].Http ://www. ietf . org/html . charter/manet - charter. Html,1997.

Zhou L D, Hass Z J. Securing Ad Hoc networks[J]. IEEE Nerworks Special Issue on Network Security, 1999, 7(06):24-30.