云计算平台的虚拟安全

陈鹏福[1] 梁正平[2] 宋佳佳[2] 陈剑勇[2]

[1]（ 中国科学院深圳先进技术研究院 深圳 518000 ）
[2]（ 深圳大学计算机科学与软件工程学院 深圳 518000 ）

摘 要 随着信息技术的发展和环保节能技术的普及和深入人心，越来越多的个人和组织对虚拟化技术感兴趣。然而，敏感数据传输和在线存储的安全是虚拟工作面临的重要挑战之一。在本文中，我们提供一个新的运行在云计算平台上的安全服务解决方案，该方案使用虚拟专有网络（VPN）和透明加密方式来保护虚拟工作的安全。它的优点是：按需使用，方便易用，成本效益高和管理简单。可以为中小型企业节省开支，不需要采购IT设备建立自己的虚拟工作的安全解决方案。

关键词 云计算；虚拟专用网络；文件系统过滤驱动；透明加密

Virtual Working Security on Cloud Computing Platform

CHEN Peng-fu[1] LIANG Zheng-ping[2] SONG Jia-jia[2] CHEN Jian-yong[2]

[1] (*Center for Cloud Computing, Shenzhen Institutes of Advanced Technology, Shenzhen* 518000, *China*)
[2] (*College of Computer Science and Software Engineering, Shenzhen University, Shenzhen* 518000, *China*)

Abstract With the development of information technology and attention of energy reservation, more and more people and organizations are interested in working virtually. However, security is one of important challenges for virtual working since sensitive data is transmitted and stored online. In this paper, we propose a novel solution as a security service on cloud computing platform to protect virtual working with on-demand virtual private network (VPN) as well as transparent encryption. Advantages of the solution are on-demand, easy to use, cost effective and simple management. It can also save expenditure for small and medium-sized enterprises which needn't invest IT systems to set up their own security solution for virtual working.

Keywords cloud computing; VPN; file system filter driver; transparent encryption

1 Introduction

Nowadays, many cities in the world are becoming larger and larger. More and more people stay far away from working place and have to take more time on the way to it. On the other hand, with the development of globalization, more and more companies, even small companies, have to open different branches in different countries. Collaboration among the branches is one of enormous expenders. Virtual working is becoming one of important solutions to save energy resource and improve working efficiency. One of main advantages for virtual working is that people can work with a team at any anywhere. They can work together virtually even if they are located in different places, such as office, hotel, airport and home.

Traditionally, one company can buy server systems to set

作者简介：陈鹏福，中科云计算领域的企业董事、常务副总经理，拥有国际电信运营商最高级技术认证CCIE（Cisco Certified Internet Expert），曾担任大型国企政企客户部网络工程师，拥有大型政府企业网络的设计部署经验，近年来从事云计算领域智能企业管理系统的研究探索，与新加坡成功企业家李先生合作创办企业，进军中国互联网市场专注云计算领域，参与第十三届中国国际高新技术成果交易会及中国计算机大会，荣获“优秀产品奖”；梁正平，博士，副教授，主要研究方向为软件工程、计算机网络、信息安全、算法分析与设计、形式化方法与技术等；陈剑勇，博士，累计以第一作者发表SCI收录论文24篇，其中属于JCR 1区（Web of Science JCR分区）论文10篇，累计获已授权发明专利24项，牵头起草国际标准3项，国家通信行业标准1项，2011年获广东省标准创新贡献奖1等奖（作者排名第一）；宋佳佳，硕士，研究助理，主要研究方向为云计算、智能网络等方面的研究。

up infrastructure of virtual working for their employees to work virtually. However, it needs a lot of investment including equipment and daily management. For small and medium companies, it is not an economic solution. Virtual working on cloud computing can evidently cut down the cost since the service is on-demand and the infrastructure of cloud computing can be shared among various companies. However, once the virtual working is built on cloud computing that is managed by the third party, security becomes a serious issue because sensitive data can't be fully controlled by the owner. Since the sensitive data is transmitted and stored online, security is key issue that may hinder the popularization of virtual working on cloud computing. Protection of sensitive data in transmission and storage is two important segments of security solution where virtual private network (VPN) and data encryption are used.

Regarding VPN, IPSec VPN and SSL VPN are the two most common protocols to be used in Internet [1, 2]. Nowadays, since many local networks use private IP addresses and connect with Internet with Network address translation (NAT) [3], it is hard for IPSec VPN to provide end-to-end VPN connections because of the complexity of setting up and management. The SSL VPN is easier to be set up and used than IPSec VPN, but it is limited to the web applications. For C/S structure of the non-Web system application, the SSL VPN requires additional configuration and technical support. For instance, it must carry on the pointed disposition in the server and the client needs to install the miscellaneous plug-ins, which bring inconvenience to application and deployment.

Regarding data encryption, there have been many reports on data security in distribute storage and remote storage. Secure decentralized erasure code is proposed to protect privacy data in distributed network storage [4]. A third party auditor is used to secure cloud data storage in the Cloud Computing [1, 2]. For the remote data storage, a stackable file system layer is designed to provide secure file sharing over remote untrusted storage systems [5]. Although these solutions for data encryption can be used in virtual working, user should decrypt the data before using it. It is difficult to be used by users who are not experts of computer technologies.

Security for virtual working on cloud computing requires on-demand characteristics and is easy to use for users. Moreover, since data in transmission and in storage are two alternate status of virtual working in cloud computing environment, it is necessary to protect data in the two statuses with an integrate security solution. To address these issues, we developed an integrated solution based on on-demand VPN and transparent encryption. What is different with traditional VPN is that enterprises no longer need to purchase and deploy the VPN system and encryption data are transparent to legal users. They can build an end-to-end working platform through renting virtual VPN as well as the data security service. The fundamental contributions of this article include the following aspects:

- Proposing a general security architecture for virtual working on cloud computing.
- Developing transparent encryption technology which is based on File System Filter Driver (FSFD).
- Designing VPN tunnel with combination of authentication cloud and relay cloud.

The rest of this article is organized as follows. We present security architecture of virtual working based on cloud computing platform. We provide transparent encryption technology to encrypt all data on virtual working, i.e., data in storage cloud, data in transmission and data in client. We further design authentication cloud and relay cloud to set up connection among clients and their connections to the storage cloud. The integration of transparent encryption, storage cloud, authentication cloud, relay cloud can provide virtual working securely. Finally, we conclude this article.

2 Security Architecture

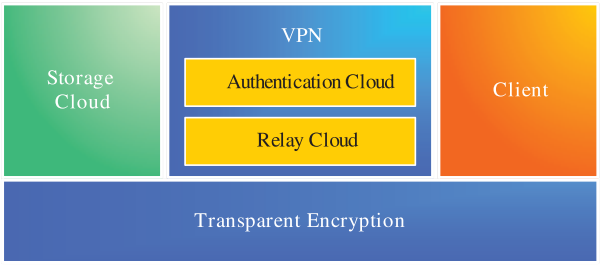

Figure 1. Security architecture of virtual working

Security architecture of virtual working is shown in

figure 1 which is divided into two layers. The first layer is transparent encryption which encrypts all data on virtual working, no matter the data is in storage cloud, clients or in transmission. The second layer has storage cloud which stores online data for clients, VPN tunnel which set up connection among clients and the storage cloud, clients which are interface channel between cloud platform and users. The client can be thin client which is only interface channel between cloud computing and users. It can also be thick client which can store part of user data and install service software to execute service.

The functional entities for the security architecture are shown in figure 2. There is an agent in every client which executes authentication, file transparent encryption and network connection.

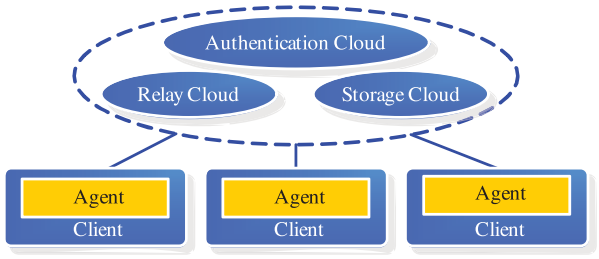

Figure 2. Functional entities for security architecture

In the cloud computing side, there three types of clouds, i.e., authentication cloud, relay cloud and storage cloud. The authentication cloud deals with authentication requirement from agents which decide the acceptance or rejection of access from clients. The relay cloud tries to set up and maintains dynamic connection with the agents. The storage cloud is a container that stores data with file transparent encryption from the agents. The file transparent encryption guarantees data security in both storage and transmission processes. Cipher text may be stored only in client or cloud storage, or in both of them that depends on application requirements. In transmission process, VPN can be realized with the dynamic connection combing with file transparent encryption for data. The security architecture is simple and flexible which can meet with complex network environment of virtual working. In the following, we firstly present the transparent encryption model in detail and then present the VPN.

3 FSFD-based Transparent Encryption Model

In the above security architecture, transparent encryption is mainly used to ensure the security of the sensitive data in both storage stage and transmission process. Moreover, it has the characteristic of mandatory and automation, which is transparent to the user and needn't change users' operation habit.

In this paper, we adopt FSFD technology to perform transparent encryption. Between I/O manager and file system drivers, a non-device driver named FSFD is inserted. A FSFD is an optional driver that adds value to or modifies the behavior of a file system. It is a kernel-mode component that runs as part of the operation system executive. The FSFD can filter I/O operations for one or more file system that is outstanding with its efficiency and stability.

3.1 Transparent Encryption Model

Transparent encryption model is designed with two layers. One is application layer and the other is kernel layer, as shown in figure 3. In the application layer, there are three important modules, i.e., application control module, key management module and identity authentication module, which are defined as follows:

3.1.1 Application control module.

On the one hand, this module is responsible for data exchange with all modules in application layer, such as getting authentication result from identity management module, getting keys from key management module and updating key to it, and constituting security strategies to security strategy module according to customer needs. Among them, security strategies including directories and file types are monitored [6]. On the other hand, the application control module is responsible to communicate with the kernel layer. It sends instructions to FSFD module with starting or stopping codes, control code, and encryption key. It also receives operation result from the FSFD module.

3.1.2 Key management module.

This module deals with key storage, key classification and key update.

3.1.3 Identity authentication module.

This module is used to verify the legitimacy of user

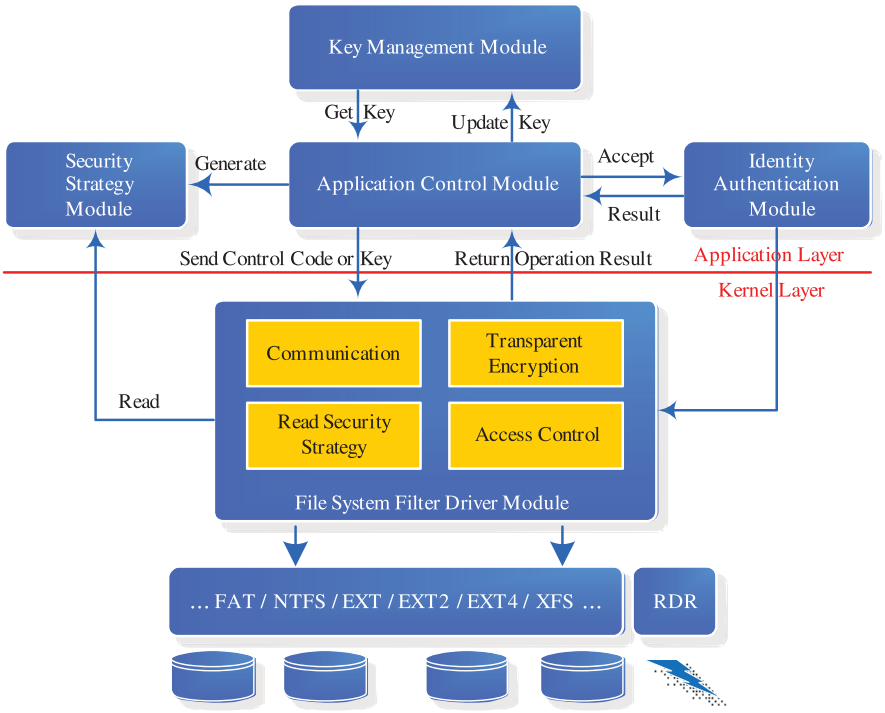

Figure 3. Transparent encryption model

identities, and returns the results to application control module.

In the kernel layer, FSFD module is core of the whole layer. It intercepts I/O Request, implements all kinds of security strategies set by users, controls access connections and executes transparent data encryption. Besides, it provides various interfaces for the application control module.

3.2 Transparent Encryption/Decryption

The technology to achieve transparent encryption is base on FSFD. The main idea of FSFD is to add a filter layer between I/O management and file system. This filter layer can catch I/O request from application layer to do additional encryption or decryption. It only catches two type of I/O request, i.e., read and write.

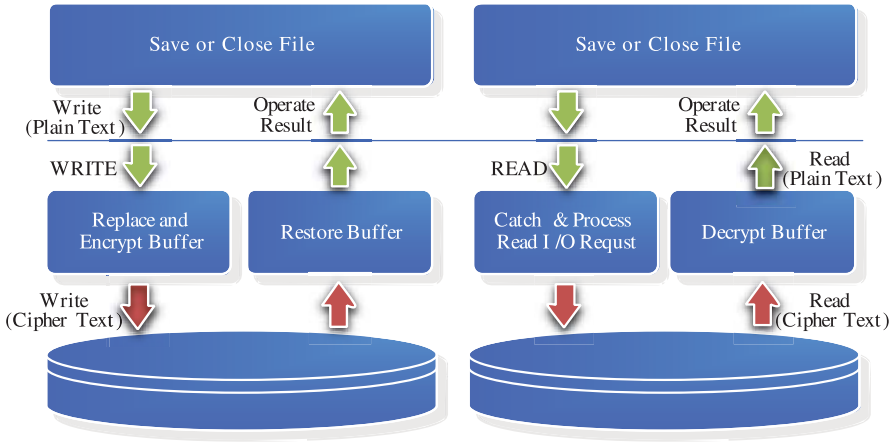

Figure 4. Transparent encryption/decryption flow chart

Figure 4 shows transparent encryption/ decryption flow chart in FSFD module. When the file data is written to disk, it intercepts WRITE operation, gains the file data buffer and then encrypts it. Note that if the writing buffer can't be modified, it is necessary to allocate an additional buffer to replace the original one. In this case, the original buffer is saved, and the additional buffer is assigned for writing process. If the WRITE operation is completed, the additional buffer replaces the original one. When the application reads the file data from disk, the filter driver

intercepts READ request, and decrypts buffer data before it is be returned to application procedure[7].

Moreover, the management of data buffer is very important. Although the data is encrypted and written to disk successfully, there may retain a copy of it in the system buffer with plain text. If the data buffer is not protected, it is easily to leak information. Therefore, when file encryption completes or the data in buffer is no longer useful, the data in buffer should be cleaned out as soon as possible [6].

3.3 Encryption Tag

Usually, the encryption tag is a data structure which records type of encryption algorithm, length of file for encryption, name of company and other identification information. It is mainly used to distinguish whether a file has been encrypted or not. There are two places to store the encryption tag, i.e., outside the encrypted file and inside the encrypted file. In the former case, the encrypted files cannot be decrypted when encryption tag lost. Therefore, it is better to store encryption tag inside the encrypted file that can compatible with all known existing file systems.

3.4 Virtual Private Network

For virtual working, it is necessary to set up VPN among clients which belong to the same group, such as the same company or the same team. With the aid of transparent encryption mechanism, VPN can be set up by the connections of clients within a group which is taken by the authentication cloud. This paper proposes dynamical connections among clients which are performed by both the authentication cloud and relay cloud. The authentication cloud takes charge of registration and authentication of every client who want to connect to the cloud platform. The relay cloud takes charge of data transmitting among clients which have already been authenticated by the authentication cloud. Figure 5 shows the framework of dynamical connections with the cloud computing platform.

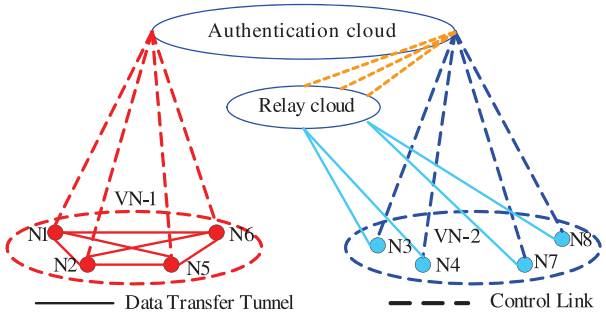

Figure 5. Framework of dynamical connections with the cloud computing platform

In figure 5, clients N1, N2, N5 and N6 have already registered to the authentication cloud as a group. After the authentication cloud authenticates them successfully, they can form a VPN named VN-1. Similarly, clients N3, N4, N7 and N8 are the same group and register to the authentication cloud. They can form another VPN named VN-2. Authentication cloud only deals with dynamical connections among clients which are maintained by control link. For virtual working, we need use the VPN to transmit cipher text among clients. Normally, once the connection is set up, the cipher text can be transmitted with point to point (P2P), i.e., from client to client directly. However, the access network scenarios for various clients are always complex for virtual working because it should allow people to use the virtual working systems in anywhere where the client can up link to Internet. In some cases such as clients locating in Intranet with private IP address, it is impossible to transmit cipher text with P2P. The private IP address of clients should be transformed to public address by NAT/CGN equipment In this case, the transmission should depend on relay cloud which can help both sides pass through NAT equipment. For example, in figure 5, clients of VN-2 locate in different Intranet. They transmit cipher text through relay cloud.

4 Application Scenario

A typical deployment of cloud-based virtual working solutions is shown in figure 6.

In this figure, clients uplink to cloud computing platform from various network access scenarios, such as home (N1), office (N3, N4, N7 and N8), hotel (N5) and airport (N6). Firstly, all clients register to authentication cloud and are organized as members of the same company. When they want to use the virtual working tool, they login to the authentication cloud with username and password. Since they are members of the same company, their connections are within the same VPN. Every client reports its own network attribute to the authentication

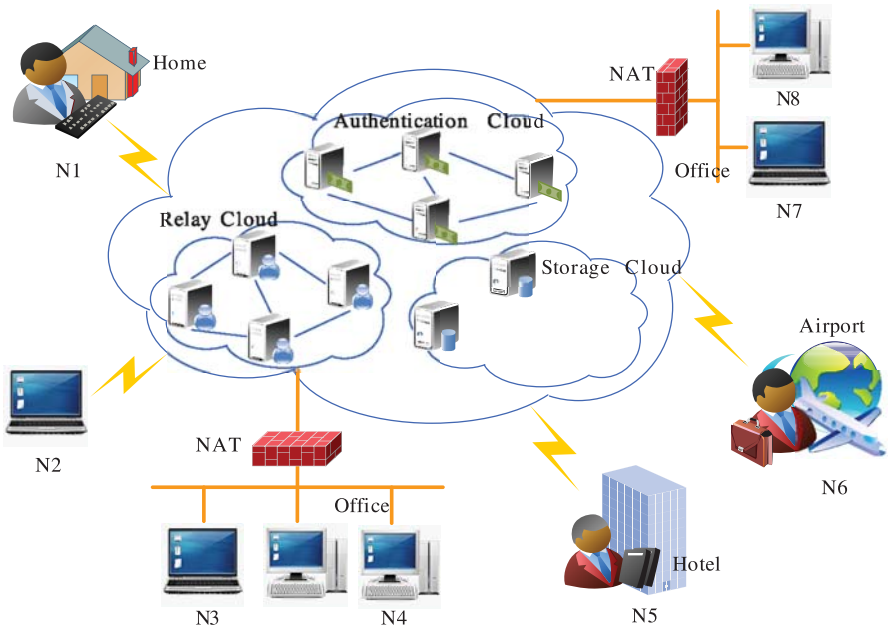

Figure 6. Application scenario of virtual working

cloud, such as the current IP (Public IP, or Private IP) address and the port used by the agent in client terminal. The authentication cloud records the network attribute of all the online clients. In this way, any online client can get network attribute of other online clients in the same company from the authentication cloud. If a source client want to contact with a destination client, it gets network attribute of the destination client and tries to establish direct connection between them, i.e., point-to-point (P2P) connection. If the clients are behind the NAT (IP network address translation) equipments, such as N3, N4, N7 and N8, it is impossible to set up P2P connection directly. The cipher text should be relayed by the relay cloud which can help both sides of clients to communicate each other. After the connections are established, both sides can transmit cipher text because all the data among clients has already been encrypted by the transparent encryption technology. If more than two clients need communicate together, such as VoIP conference, the relay cloud can take as a common bridge to deliver data among them. If client wants to connect to storage cloud, the storage cloud acts as destination client and the connection can also be established according to above framework. Therefore, all clients in figure 6 can securely work virtually with their colleagues at any place where they can uplink to the internet. For small and medium companies, they needn't buy IT systems shown in figure 6. Cloud computing provider provides these IT systems. What companies do is to register as a group of users in the cloud computing. Then all the staff can join the virtual working securely once their clients can uplink to Internet. The company need only pay for it according to application amount.

5 Conclusion

Based on transparent encryption for all user data, the solution uses authentication cloud, relay cloud and storage cloud to set up security architecture for the virtual working. We use FSFD based technology to perform the transparent encryption. Based on the transparent encryption, we further use the combination of authentication cloud and relay cloud to set up VPN tunnel for the virtual working solution. It is on-demand, easy to use, cost effective and simple deployment and management. Based on cloud platform, it can also save expenditure for small and medium-sized enterprises which needn't invest IT systems to set up their own security solution for virtual working.

Acknowledgment

The work was supported by China-Finland Cooperation

Project on the Development and Demonstration of Intelligent Design Platform Driven by Living Lab Methodology (2010DFA12780), and Science & Technology Fund of Shenzhen (JC201005250045A, JC201005280432A).

References

[1] Wang C, Ren K, Lou W J, et al. Toward publicly auditable secure cloud data storage services [J]. IEEE Network,2010, 24(4): 19-24.

[2] Wang Q, Wang C, Ren K, et al. Enabling public auditability and data dynamics for storage security in cloud computing [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847-859.

[3] Kubota A, Miyake Y. Public key-based rendezvous infrastructure for secure and flexible private networking [C] // IEEE International Conference on Comunications, 2009.

[4] Lin H Y, Tzeng W G. A secure decentralized erasure code for distributed networked storage [J]. IEEE Transactions on Parallel Distributed Systems, 2010, 21(11): 1586-1594.

[5] Geron E, Wool A. CRUST: cryptographic remote untrusted storage without public keys [J]. International Journal of Information Security, 2009, 8(5): 357-377.

[6] Ling J, Li J Z. An improved security technique for the terminal sensitive documents [C] // International Conference on Computer Sciences and Convergence Information Technology, 2010.

[7] Microsoft. Filter Driver Development Guide [Z]. 2004.