Cloud Computing Environment Analysis of the Electronic Evidence Forensics Key Technology

Ping Teng
Liaoning Police College, Dalian,116036,china

Keywords: cloud computing environment; electronic evidence; evidence; the key technology

Abstract: Cloud computing refers to the computer storage, application and service ability combined with the user needs to be allocated, which not only provides high quality services for customers, but also reduces the user software purchase cost of a new kind of calculation method. However, in view of the cloud forensics, it belongs to a new field development, therefore, to severely crack down on Internet crime, it is necessary to explore a set of more perfect survey methods. In this paper, the electronic evidence forensics definition of cloud computing environment as well as the application of key technologies are analyzed in detail. It is hoped the technology can provide some references.

1. INTRODUCTION

In recent years, due to the popularity of the Internet technology development, making illegal destruction of the computer system, network theft and other new type of crime continues to increase. And, in the detection of computer network crime, make use of email, data exchange as its evidence, such as, funds transfer, web become an essential part of. Thus, through the electronic evidence forensics technology and law, statistics and other disciplines are closely combined, inevitably to solve computer network crimes have a positive impact.

2. SEVERAL KEY TECHNOLOGIES ABOUT ELECTRONIC EVIDENCE COMMONLY USED

Electronic evidence refers to using technologies such as electronic, electromagnetic or optical storage in computer, magnetic materials, or optical devices to prove that a criminal case in the actual situation of all the data information. But in recent years, because of the computer technology and network technology is developing towards complicated, the traditional through closed system of the computer system for hard disk image method is difficult to meet the demand of the current evidence. At present, the electronic evidence is the rapid development in the direction of the electronic network forensics. Electronic forensics technology, however, the criminal techniques and methods of change, is developing toward the direction of diversification, so, electronic evidence must be made of high-end technology as support. The author aimed at several key technologies commonly used in electronic evidence in detail (Xia, 2011).

2.1 The Data Replication Technology

This technology contains a variety of forms such as mirror, photo and video. For audio-visual material evidence, for example, we can form the forensics process using pictures or video record, enhance the proof strength, to prevent crime personnel confession. After the crime, in the form of data mirroring fast backup to other computer, through the analysis of the image, far more than on the original directly operate much safer.

2.2 Information Encryption Technology

To ensure the security of data information, we often use information encryption technology. The technology refers to with the help of the key technology, is used to protect the public communication network in data transmission, exchange and storage integrity. And it is the most basic secure network communication technology.

2.3 Data Recovery Technology

The technology refers to the degree of damage or invisible area data recovery. In general, most of the computer system has function of automatic generation of backup data and restore the data. And in a security system on the basis of the system will automatically to backup the important database. The system is usually made up of some special equipment, technology and operation management, therefore, others secretly tampering with the difficulty of the system is larger. So, if after the computer crime, the system of some important data are destroyed or modified, the backup data and comparative analysis of the destruction of data to be finalized for strong evidence.

2.4 Data Capture Technology

Is this technology is to point to in the case of computer crime, to detect personnel by adopting some technology to intercept the criminal evidence of a technology. Its essence is through the transmission medium to obtain evidence of crimes. Among them, the data in the transmission, there are two main forms, namely cable transmission and wireless transmission. Among them, cable transmission technology refers to using network monitoring technology, the host network adapter pattern is set to mixed type, then seized some important data information in the process of communication. However, for the wireless transmission technology, mainly by means of electromagnetic wave to intercept the important data information in the process of communication.

2.5 Data Deception Technology

Generally speaking, the common data deception includes two kinds, namely the camouflage and trap. Among them, for camouflage methods, generally, a virtual environment system was established and induction of attack to attack it. And this way is often used in attack people obtaining evidence in the network attack. Personnel under the premise of no knowledge, the attack will camouflage in the network forensics system full records against all the operation process. In addition, the trap of the most commonly used tools include honeypot and honeynet.

3. ABOUT CLOUD COMPUTING ENVIRONMENT ANALYSIS OF THE ELECTRONIC EVIDENCE FORENSICS KEY TECHNOLOGY

3.1 Definition of Cloud Computing

In recent years, due to the electronic commerce technology, the rapid development of Internet and digital city technology, thus gradually appear the "cloud computing" model. In the United States, the following definition of cloud computing: it is actually a kind of new computing mode, main technology combined with their own needs, at any time via the Internet to access a Shared resource pool.

In our country, the famous expert in cloud computing to the following definition of cloud computing: it task distribution in the computer made up of a number of computer resources pool, this system can according to the computing power, storage, and software application services.

Because the current about cloud computing is not a unified definition, therefore, the domestic scholars to a general description of cloud computing. By the user to understand the definition of cloud computing: it refers to the combination of user requirements to computing power, storage capacity, service capacity and reasonable assignment, the final purpose is to provide convenience for the user, at the same time reduce the overall cost of the users to buy the software and hardware (Ding,2011) .

3.2 Cloud Key Techniques in The Environment of Electronic Evidence

3.2.1 Cloud Computing Technology Needs to Solve Technical Problems

Before using cloud computing technology, the first thing to solve the following three questions:

- how to create a good environment for cloud computing

This problem belongs to build a cloud platform at the bottom of the problem. For cloud infrastructure providers, it corresponds to the IaaS layer. At present, still have a lot of problems need to be solved, such as: programming mode, cloud security, monitoring, resource management and scheduling, etc.

- how to realize the cloud services

Combined with the problems, as a cloud application developers, to achieve the purpose of application, the corresponding service must be deployed in the cloud. And we have the problem to be solved by the cloud provider facilities provided by the API, to develop a cloud service can satisfy various customers' needs.

- how to use cloud services

For users of cloud computing, because the data and services in the cloud, so that the user does not need to considering to terminal facilities requirement, but against YunPing Thai charge, security and service quality problems such as comprehensive consideration. However, should be noted: different types of users in the face of different levels, is not corresponding to each other, this is due to the users in the use of cloud computing, the body can be converted.

3.2.2 Cloud Architecture Development Technical Problems

- to achieve the unity of the exchange schema

In order to reach the unity of exchange architecture requirements, must use more advanced technology. One of the most representative technique involves: Ethernet technology, Ethernet fibre channel technology. At present, the Ethernet data transmission can achieve Wan Zhao above, and the Ethernet performance is higher than ever, the delay time is more short.

- to achieve reunification of the virtualization mechanisms

According to the analysis of the definition of cloud computing definition, must want to build a data center. But, for server virtualization, it refers to using virtual machine migration eventually achieve the goal of physical resources sharing or copy. And that we must build a unified virtual mechanism in advance.

- to realize the unification of the computing system

The final realization of cloud computing, depending on system integration and management components, such as: computing components, storage components, etc. This can greatly reduce the cost of ICT consumption, and can reduce the complexity of the cloud computing system, make the ICT has high flexibility, better meet the diverse needs of social development in the future.

4. UNDER THE ENVIRONMENT OF CLOUD FORENSICS USAGE AND PROCESS

4.1 Forensics Usage

4.1.1 Survey

First, to the violation of multiple jurisdiction or multi-tenant cloud computing environment investigation; Second, the survey of operation, the cloud response of the system event; Third, to construct the cloud events; Fourth, provide strong evidence for court and government; Fifth, to cooperate with more evidence.

4.1.2 Troubleshooting

For fault data file for possible location, at the same time in a cloud environment to the related document to track; Development trend about one event shall be determined, and then develop over time, find the reason that affect other events, at the same time improve the coping strategies, avoid the occurrence of similar events;

Events in cloud computing environment conditions in tracking and evaluation; Timely and effective handling all kinds of accidents happened in cloud computing environment.

4.1.3 Data Recovery

When a cloud environment destroyed by others or delete data information, must carry out data recovery; When the encryption key is missing, must also be to restore the data.

4.2 The Forensics Process

In a cloud environment, evidence must be conducted according to the following several steps: first, the cloud forensics aims to determine; Second, determine the type of cloud forensics; Third, the technical background type shall be determined; Fourth, the use of special execution of forensics tools to collect user information; Fifth, server and cloud service providers to be communication and exchanges, collecting suppliers cloud service information; Sixth, by the cloud service developer divide end to collect relevant evidence; To upload data using tools to determine; Time is consistent with the cloud service provider (Wu, 2011).

5. CLOUD COMPUTING ELECTRONIC FORENSICS TECHNOLOGY DEVELOPMENT DIRECTION IN THE FUTURE

Due to the rapid development of computer technology and information security technology, so as to make the electronic cloud forensics will be rapid development in the direction of the automatic and intelligent; Cloud forensics tools more professional development; Compiling unified cloud electronic forensics specifications and standards; Sound on cloud forensics laws and regulations; Cloud electronic evidence gradually evolved into a cloud services; Close combination of static forensics and dynamic forensics, open up a new prospect for development cloud forensics. In addition, the work and many places need to be corrected, and even some places need to be verified. Mainly includes the following three aspects: first, the current cloud computing environment of forensics model is not very perfect, and evidence for subsequent analysis and performance are not described in detail; Second, at present, for the migration method considering the cloud computing environment is to ensure that the data is consistent with the implementation process. Migration methods, however, did not consider about judicial authentication work, therefore, must be in the future research work to further strengthen the legal efficiency of forensic authentication; Third, because of the cloud computing environment is more complex, so the need to strengthen in terms of system suitability. Of electronic evidence, however, because of the cloud computing environment for a new type of evidence of thinking, so that we can be bold attempt to obtain evidence environment, to expect in the future work to improve gradually.

6. CONCLUSIONS

A lot of new challenges, in general, the development of cloud computing is, but because of the lack of corresponding policies and standards, so that make cloud computing is faced with new challenges. In addition, because of the rapid development of network technology, which leads to the traditional computer forensics tools to better meet the needs of the current electronic forensics environmental changes. Especially in cloud computing environment of forensics work, must with the aid of a large number of advanced technology or method. The cloud, so to speak, is usually composed of a distributed heterogeneous virtual computing resources, data can be shared by several users at the same time. And most likely to work relationship between them, it is also possible to provide services, resulting in a user temporary access records. However, in such a complex environment of complete electronic forensics work, is difficult to achieve. But in a cloud computing environment, it is entirely possible to crack down on Internet crime forensics work possible. So, in this paper, the author for the electronic evidence forensics definition of cloud computing environment as well as the application of key technologies are analyzed in detail. Hope can provide some reference and reference. At the same time, the forensics work under the cloud computing environment for the future to provide some reference data. And make a certain contribution to crack down on Internet crime.

REFERENCES

[1] Xia, R., 2011. Cloud computing technology application research in the field of electronic data evidence. *Information Network Security*. 13(8), pp.113-113.

[2] Ding, Q.F., 2011. Cloud computing environment forensics technology research. *Information Network Security*. 17(11), pp.145-145.

[3] Wu, S.B., 2012. Cloud computing environment of the electronic evidence forensics key technology research. *Journal of Computer Science*. 33(3) 6, pp.138-138.