Study on Investigation and Forensics by Computer under Cloud Computing Environment

Sun Cui
School of Economy and Management
Shenyang Aerospace University
Shenyang City, China

Abstract-Today's Internet technology becomes more advanced. Computer has been increasingly applied in all aspects of the society, and we will continue to increase and expand. In the continuous development of computer applications, a lot of problems are emerging, in which using computer as a means of theft or damaging others are common. It not only brings a lot of security risks for people's lives but also brings more and more social harm. In mass of information in the network, if you want to investigate who using what kind of means to do cybercrime precisely and effectively, the traditional forensic techniques cannot meet our needs. Therefore, in computer crime investigation, how to identify computer crime and how to get the evidence is still a problem worthy studying.

Keywords-Cloud computing environment; Computer investigation and forensics; Problem study; Countermeasures

I. INTRODUCTION

With continuous development and progress of computer technology, a variety of new concepts also developed, in which "cloud computing" has become trendy in recent years. It's also relatively revolutionary new concept in computer technology. The computer technology under cloud computing environment is becoming more and more mature through continuous reform and improvement.

Introducing cloud computing environment into the field of computer investigation forensics is a model of computer development, which can help people to track and confirm computer crime personnel, bringing great convenience for computer investigation and evidence collection. This paper focuses on analyzing the technical crime forensics under computer cloud computing environment and simply mentions some countermeasures.

A. What is cloud computing environment?

Concept of cloud computing environment: The so-called cloud computing environment refers to a new business model following the service computing and network computing, which is based on Internet-related services increasing, usage and delivery models, usually involving internet providing dynamically scalable and often virtual resources. Also it's an integration and development of computer technology and network technology. The application of cloud environment is different, so its concept is a little different due to different people and organizations, but in general, the core of cloud computing is to finish the computing through massive data storage and computation, and then the information is reassembled and processing, and finally provide customers with the results through network [1].

B. Features of cloud computing environment

(A) Accurate, objective, and reliable. There is a lot of data being store in cloud computing. Multiple copies fault-tolerant, computing nodes isomorphic interchangeable and other measures can guarantee the high reality of service, which makes the possibility of errors under cloud environment greatly reduce, and therefore cloud computing is more reliable than local computer.

(B) System virtualization. Cloud computing environment users require corresponding service, rather than focusing on the underlying information on behind of services. Cloud computing system supports users to get the applications and services they want in any location, any terminal, therefore, it will make each resource virtualized to meet the different needs of users [2].

(C) Super-large scale high scalability. Cloud computing itself has a fairly large scale, millions of servers making cloud computing have unprecedented ultra-high computing power. Super-large scale of "cloud" in providing computer resources determines the cloud computing environment can be scalable based on the user's needs, which means that customers use in a cloud computing environment also has high scalability [3].

（D) On-demand services at any time. When the user needs service under cloud environment, they can apply in cloud computing services based on their own needs. Such an application does not need too much payment once or purchase other necessary hardware facilities, but pay according to time of service or other factors, which is a very convenient and cost-effective manner for individuals or businesses with not too big demand.

(E) Potential risk. In addition to providing computing service for the public, cloud computing services also provide a variety of corresponding storage services. This storage service has no unified management personnel, so for criminals on the network, it has a very big temptation. They will use a variety of techniques of information to

leak the information stored in the cloud service, which may cause a lot of unnecessary trouble and social impact.

II. THE PROGRESS OF COMPUTER FORENSIC TECHNOLOGY UNDER CLOUD COMPUTING ENVIRONMENT

The so-called investigation and forensic refers to the searching and judging work in detection process of a criminal case. In general, traditional investigation forensics is relatively in a sealed environment, with known or more explicit clues to analyze the forensic target. In this environment, substantially there is no interference from other data. Once the trail is not clear, then the forensic will be a difficult job. However, computer forensics under cloud computing environment is an upgrade of traditional way, and because it is constituted by a large number of clients, a variety of data sharing, users can coordinate the work and help each other, so computer forensics under cloud computing environment can get more clues and evidences than the traditional way and easier.

III. IMPLEMENTING WORK OF FORENSIC UNDER CLOUD COMPUTING ENVIRONMENT

Under cloud computing environment, the realization of forensic can be divided into 3 steps: find evidence, fix evidence and extract evidence.

A. Analysis of finding evidence.

No matter what kind of environment, if there are any behaviors and actions, both crime and usual behaviors will leave various trace in the objective environment, which is also available for computer. And finding evidence is the computing of these traces. These traces leave massive information. If you want to find the evidence, you need to analyze them case by case. However, cloud computing environment have certain recording for computer using trace, which can be seen from following points:

Firstly, proceed from the cloud to find the operator of the computer directly. In the cloud computing environment, a lot of the behaviors from the user is done directly on the computer, therefore, in the search computing, it's likely to find the text, pictures, tables or other direct information used by the operator. The data user is bound to perform a number of related operations that will leave more detailed records in the database of the cloud computing, so, we can find the time used by the operator, account information through cloud forensics. And the forensics persons can directly get this part of nodes from cloud terminal, to get the operator's identity information, and obtain the corresponding illegal evidence.

Secondly, proceed from the client; discover the cache information in the computer terminal used by user. There is a lot of data passed over the network under cloud computing environment. The information will eventually be exploited by customers, so the client will store caches information delivered within a certain time, although some information is cached for a short time, but this is still more direct evidence reflecting the operational behavior of computer users.

Thirdly, investigate from information flows recorded by the service provider of cloud client. No matter public or private cloud client, domestic operators or domestic operators, the existence and operation of cloud clients must be legitimate, so we can take advantage of the left records of users in the cloud client, combining with its operators with the cloud, the user's query record evidence, for example, a computer user's IP address, login query time, the content or the address information sent and so on, these will be helpful for the discovery of evidence.

B. Fixed evidence analysis

After being found, the evidence should be timely maintained and fixed, to ensure the objectivity and integrity of the evidence. Before any kind of evidence is extracted, make sure clues and direct evidence cannot be artificially modified or polluted. Therefore, after the discovery of evidence, first thing to do is to keep the contents of the data, and focus on preservation of its peripheral electronic information and let the relevant personnel to make digital signature or witness evidence and other ways to fix the evidence in order to ensure the evidence objectivity and being used.

C. Analysis of extracting evidence

After the evidence being found and fixed, what the forensics staff needs to do is to extract the evidence. Effectively extracting of evidence determines whether the evidence can be used rationally. Evidence extracted with computer is different with the evidence extracted with the traditional way. The traditional evidence extracting is to retain or photograph prevailing circumstances, and computer evidence extracting under cloud environment may exist instability data access, and the evidence to be extracted may be contaminated. Also, the evidence may exist in more than one client, and a number of other issues, which determines evidence extracting will need a lot of bandwidth and time. Evidence extracting is to ensure the completeness of evidence. It also needs to extract neighboring data with massive data as auxiliary [4].

IV. NEW PROBLEMS FOR COMPUTER FORENSIC TECHNOLOGY BROUGHT BY CLOUD COMPUTING ENVIRONMENT

There are some changes for computer crime under cloud computing. The flexibility of cloud computing environment makes crime forensics easier and also generate huge effect for information safety, including the following aspects [5]:

A. Problem of forensics technology

Firstly, the technology development is out-dated and not timely, which cannot meet the needs of forensic technology. Out-dated forensics technology has been a major issue for China. By comparison, we found that out-dated technology is mainly resulting from technology development behind. The computers mostly used in China are set for local computer, and these computers are enough for local computer data recovery, cache and operation logs. These updates rely on the software bought sometimes or other ways, and cloud computing environments are in large network environment, which has higher requirements for network packet, server node , resulting in

our local computer design technology is completely incompatible with the needs of cloud computing, data packet. The information analysis technology of server node is not in place, and the development is not timely that cannot meet the needs of forensic technology.

Secondly, the forensic staff lack of appropriate technical quality and skills, thus failing to ensure comprehensiveness and integrity of information. When there are new forensic techniques, if the forensic staff cannot improve their technical quality, it is impossible to effectively play the role of high-tech. At the request of cloud environment, forensics technology is not just for static data storage, also for dynamic encoding, the only way to combine with the investigation, to ensure the full integrity of evidence information.

B. Issues on forensics laws

Forensics under cloud environment is mainly to combat and prevent crime behavior, so it is a legitimate activity itself, so it should be protected by law and in accordance with law. Now, our current law is not perfect in this regard, even exists a lot of problems: First, China's criminal law is ill-defined for the types of crime, which leads the crime cannot be punished by existing laws after obtaining the evidence.

Secondly, because the servers of cloud computing may belong to different service operators, the span of area will be relatively large, and in the span of the area, there is no legal protection of rights, resulting in legitimate forensics more difficult.

C. Cooperation issues between forensics organizations

Under cloud computing environment, when different service clients are required for forensics, usually they cannot communicate and cooperate due to respective benefits, which including two aspects: firstly, refusing to cooperate with other clients with privacy right as excuse. Secondly, taking business secret as excuse to refuse cooperate with forensics organizations and other service providers.

V. COUNTERMEASURES OF COMPUTER FORENSICS ISSUES UNDER CLOUD COMPUTING ENVIRONMENT

A. Technical countermeasure

Firstly, guarantee the update of the existing technologies. Cloud computing works under relatively advanced environment, which requires that the surrounding environment and hardware, software facilities should be updated in time. After equipment and software updated, the forensics staff technical qualification also needs to be improved, unless the updated equipment and software cannot be effectively used. The way to improve the qualification of the existing staff is to strengthen training and selecting more high-level staff. Usually, the forensics staff can do self-drilling in simulative environment for examination and selection.

Secondly, strengthen self-development of technologies and communication. Because the super large extendibility of cloud computing determines the complexity, variability and uncertainty, which proves that only improving the forensics level of the existing staff is not enough.

B. *Law countermeasure*

Firstly, sound national laws and regulations. Sound national laws and regulations refer to defining forensics behavior rules, focusing on the normal specifications of forensics behaviors, to ensure laws to abide by in the forensics process and determine what kind of responsibilities should be undertaken against the obtained evidences, stipulated by the law.

Secondly, Under the provisions for individual clients without affecting the essential interests of its case, to actively cooperate with the judicial authorities and forensic staff. Normal extract forensic work. In peacetime we should establish and improve the information exchange channels between each client, so that one can communicate new information, on the other hand in the judiciary and the judiciary may also be exchanges of evidence, thus forming a tripartite joint exchanges of the situation, not only can effectively promote the development of cloud computing information technology, also can be done easily and quickly when the forensic.

Thirdly, establish relevant judicial and supervision departments. Any implementation of laws and regulations must need an impartial judicial supervision department, therefore, under cloud computing forensics environment, if there are laws to abide by and strictly enforce, related judicial supervision departments must be established.

VI. CONCLUSION

With the rapid development of technology, cloud computing has gradually spread over around us. Facing with a growing number of computer network security problems, traditional computer forensics has been difficult to meet the requirements, and therefore forensics under cloud computing environment has become an inevitable trend. Although cloud computing has undesirable disadvantages, but as long as performing continuous technological innovation and practical application, while carrying out continuous study for computer forensics to make the forensics technology under cloud computing environment further improved to ensure scientific and rational use, effectively combating computer crime, ushering the real "cloud era".

REFERENCES

[1] He Xiaoxing, Wang Jianhong. Study on Forensics Problems under Cloud Computing Environment [J]. Computer science, 2012, 39: 105-108.

[2] Liu Peng. Interpretation of Cloud Computing and Security [J]. Chinese Security, 201174-37

[3] Wu Tong, Yang Yongchuan. Forensic Study under Cloud Computing Environment [J] Telecommunications, 2010,12: 80

[4] Li Xiaokai. Study on computer forensics problem under cloud computing environment [J]. China University of Political Science, Master's thesis, 2011, D918

[5] Zhou Gang, Study on Scene Migration Technology of Forensics under Cloud Computing Environment [J]. Computer Science, 2012,39 (09)

[6] Luan Runsheng. Thinking of Computer-Oriented Cybercrime Forensics of Cloud Computing [J]. Network Security Technology and Application, 2011,12: 68

