Cloud Crime to Traditional Digital Forensic Legal and Technical Challenges and Countermeasures

Hai-Yan CHEN
East China University of Political Science and Law
Shanghai, China
tom_chy@163.com

Abstract—**With the maturing and wide application of cloud computing technology, there are more and more crimes in the environment of cloud computing. It is prospectively analyzed that the possible types of crime in the cloud computing environment. Because of the characteristics of cloud computing , the traditional digital forensics in the cloud computing application environment are falling in trouble not only in laws but also in technology, this paper analyzes the difficulties. For digital forensics work effectively fighting against crimes in the cloud computing environment, this paper presents suggestions and solutions in two aspects of legal and technical.**

Keywords- Cloud computing; Cloud crime; Cloud Forensics; Digital Forensics

I. INTRODUCTION

Cloud computing is one new computational method designed to process the Big Data, which is regarded the 3rd technological revolution of the IT industry. It used to be developed for some large-scale IT enterprises to resolve the problem of storing and calculating considerable amount of data produced by themselves. This mode was then popularized by those leading companies to offer services for enterprise which was having a hard time dealing with the big data. It altered the regular mode of how people use their computers, in the users' convenience to consider, with the aid of the cloud serving system offered by the cloud serving operator, it can meet the needs of various gradations of software and hardwire, just like using the conventional utility, helps the users to shake off the expensive expenditures on buying software and hardware to preserve the cost. These services include three main gradations: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)[1].

Since the concept of cloud computing was raised on 2007, the technology has been rapidly developed. So far, companies with service on IaaS including Amazon EC2、Eucalyptus 、Nimbus etc. Those with service on PaaS including App Engine 、Windows Azure 、Force.com 、Amazon S3 etc. Those with service on SaaS including Google Apps、Microsoft Online、SalesForce etc. A lot of enterprises such as Google、Amazon、Facebook、Alibaba use the cloud computing service system as the basis of a lot of their businesses.

Thus it could be seen that, in the near future, cloud computing will soon enter a booming stage. Along with it comes the increasing criminal activities in the cloud computing environment，as in this article we called cloud crime.

II. CLOUD CRIME AND FORENSICS

Since the cloud computing technology has been applied, on this basis, frequent criminal activities occurred over time. For instance, in 2009 'Distributed Denial of Service',(DDOS),brings cloud paralysis to Twitter; in 2009 and 2011 two large-scale incidences happened to the cloud service of Google that the user files were unconsciously slipped out, in the April of 2011 some criminals took the advantage of the powerful calculating skill of Amazon EC2 to steal credit cards from ten thousands of people; on July17th of 2011 SONY website PlayStation as well as Sony Online Entertainment were invaded by computer hacker，a massive scale of SONY MP3 and music were steeled, ultimately cause the great leakage of a large amount of users information.

Foreseeably, cloud crime will be set off in two aspects. First was to utilize the characteristic of cloud computing mode itself to launch the attack and bring about damages. Such as the Virtual Machine Escape [2], which took the advantage of the loopholes in the virtual machine software as to keep other mainframes or virtual machines under control in order to get the aim of obtaining illegal information or posing the damage? Another gigantic threat was the denial of service attack DoS and DDos[3] to the cloud computing environment which was constructed by internet. Once the attack takes effect, it would be a great challenge to communicate between the computing nodes which might cause cloud paralysis. Cloud computing can provide us with powerful computing skill, with which the assailants could easily decode various kinds of encrypted measures and files, illegally steal important information or even destroy the whole cloud system. Second was to transplant the conventional crime from the ordinary world to the cloud environment, such as Internet pornography， Network gambling，Pirated video，Phishing web site etc.

With regard to the Judicial Forensics over those criminal act, we may as well call it cloud forensics, was apparently extend of traditional digital forensics. Digital forensics was first raised by International Association of Computer Specialists（IACS）in 1991, it was also called Computer forensics or Electronic forensics in some documents, original definition was the procedure to identify, obtain,

978-1-4799-6989-0/14/$31.00©2014 IEEE

preserve, analyze and submit electronic forensics in computer, peripheral equipment and internet, the purpose was to testify criminal act and reconstruct the scene of the crime. With the development of the Information Age, digital forensics has been turned from Static Forensics to Dynamic Network Forensics and then ultimately develops into the latest state of forensics under cloud computing environment.

III. CHALLENGE TO TRADITIONAL FORENSICS

Because of the features of cloud computing such as the huge quantity of data, the virtuality of dynamic distributed storage and computing as well as the multi tenancy during runtime are largely different from the simplicity and stationarity of the traditional C/S or B/S server. Originally, the program and data of C/S or B/S server are relatively centralized storage and operation in one or a few computers. However, the service and application which constructed on cloud computing technology do not have fixed storage computer and the data was distributed among long-span computing nodes, besides, along with the increase or decrease of the storage capacity on the nodes, the phenomenon of emigration or immigration will dynamically occur; the same as the executing procedure, which was dynamically distributed, those which support the running of the program are the computing nodes which distributed among various areas(most of which use virtual machines).One computing node can install multiple virtual machines and one virtual machine can provide computation or storage service for multi-tenant application. Also with the increase and decrease of node load, dynamic emigration and immigration will occur among the running program to balance the load of each computing node, utilize the computing capacity of each computer node. This led to the situation that the traditional digital forensics technology under cloud computing environment will not be effectively applied. The laws and regulations of traditional digital forensics are in straitened circumstances either. The challenge cloud computing offered to the traditional digital forensics are mainly embodied in the following two aspects.

A. Legal predicament on traditional digital forensics work in the cloud computing environment

- The lack of regulations in substantive law

According to the NIST Cloud Computing Reference Architecture, there are five main participants: Cloud Consumer, Cloud Provider, Cloud Broker, Cloud Auditor and Cloud Carrier. In relevant substantive law in our country, the role of the five main participants in law has not been clearly defined, especially what legal liability and obligation and relevant rights they should undertake during judicial forensics. And classification of crimes in the cloud computing environment has not been defined according to relevant substantive law in our country, let alone corresponding criterion for imposing penalty, which caused some difficulties to judicial decision. Because of multi-tenancy in nature of cloud computing system, it often caused the trouble of protecting the data privacy in the process of obtaining evidence. Relevant regulations about protection of privacy right are lacked in substantive law in our country.

- the lack of regulations in procedure law

Firstly, in the procedures of obtaining evidence, laws and regulations on the process of traditional digital forensics work are imperfect and have been continuously perfect. There is a severe shortage on laws and regulations on the process of traditional digital forensics work in the cloud computing environment which newly appeared. In consideration of the huge difference between digital forensics work in the cloud computing environment and traditional digital forensics work, the original procedures of obtaining evidence can't be applied effectively.

Secondly, in the aspect of act of law on the electronic evidence, there has always been controversy on the act of law on the electronic evidence in our country and relevant laws and regulations also severely lack despite of the fact that United Nations established act of law on the electronic evidence in < UNCITRAL Model Law on Electronic Commerce> in 1996. The acts of law of electronic evidences in the cloud computing environment, which are more virtual and portable than the original data, are not illustrated correspondingly in law in our country.

Lastly, in the aspect of obtaining evidence beyond the judicial field, it is a common problem for data storage beyond the judicial field in the cloud computing environment, which led to extraordinarily difficult to digital forensics work. Currently, <Hague international convention of civil and commercial cases>, which was drew up in 1972, is wide used as regulations of obtaining evidence beyond the judicial field in the whole world, but it mainly cater to civil and commercial cases and relevant unified rules are lacked in case of case for crown. Moreover, for the reason of data's characteristic of easy-losing in the cloud computing environment, the original evidence may has disappeared when collecting evidences through other country's traditional complicated mechanism of legal procedure..

B. Technique predicament on traditional digital forensics work in the cloud

- Hardware

Traditional ways, like hard copy, memory copy and evidence storage device, can't be suitable anymore, because the original sources of evidence distribute in several virtual panel point and have a great number. It is hardly possible to copy or memory these data by right of one or several hardware. It's a hard problem to memory these original data.

- Software

Traditional software(e g. Encase,FTK)play a limited role because there's only a part of software or data in service node in the cloud services architecture in distributed virtual environment. It is a difficult problem how to obtain these distributed information sources from different cloud computing platform.

- Forensics process and technical specification

Traditional digital forensics work requires device as independent as possible, but cloud computing node equipment are shared by multiple tenants, which can't be isolated. So it's necessary that third party cloud service providers participate and relevant traditional forensics process and technical specification must be changed.

- Personnel

For the reason of the complication of cloud computing system, easy-losing of data and cross regional of Forensics, people obtaining evidence need higher professional quality. So the working standard of professional people obtaining evidence needs to be drawn up again.

- Technical means

Traditional digital forensics work can't lead to a complete acoustic image in the cloud computing environment. Data lost or deleted can be recovered in the traditional digital forensics, but once mirror stops or off the virtual machine data can't be recovered in the cloud computing environment. Ways to access to network components, like the router, load balance etc., are lacked.

IV. THE LEGAL ANSWER TO CLOUD FORENSICS DIFFICULTIES

In order to cope with challenge of the cloud crime to the traditional digital forensics, it needs to be perfected from two aspects of law and technology. Law is the guarantee and technology is the means. The two complement each other and are indispensable.

A. Improve the relevant laws and regulations

- Improve or replenish the relevant substantive laws and regulations

Currently, laws and regulations which can be used in the field of cloud crime are not very much in our country. Main laws and regulations are 《Criminal Law》, 《National Security Act》, 《The People's Police Law》, 《The Public Security Management Punishment Law》, 《The law on Guarding State Secrets》, 《The Telecommunications Regulation》, 《Decision of the National People's Congress on safeguarding Internet Security》, 《Interpretation of the Supreme People's court, the Supreme People's Procuratorate Concerning Several Issues of application of laws in the information system security of computer criminal damage》 etc.[9] But considering of specific of the cloud computing environment, the author suggests the relevant substantive law to be corrected to make the appropriate judicial interpretation.

- Establishing and completing personal privacy legislation

As the cloud computing environment has the characteristic of multi-tenant, a large number of enterprises or personal data are stored in the cloud environment, and the owner of such data cannot directly control it because the data were stored on the cloud service provider. So illegal access to the data can be quite easy, and cause the leakage of user privacy exposure or sensitive information. Many cloud crimes exposed before are of this type. So we should make it clear that the user's personal data protection in the substantive law means privacy protection as soon as possible. Any organization (including national strength mechanism) and individuals have no right to access other individuals' privacy data unless they are authorized by the data owner. Convict the criminal case of illegal access to others' privacy data according to the type and quantity of privacy data.

- Clarifying and refining the legal role of five main participants participate in cloud computing

Because the whole cloud application has five participants: cloud users, cloud service providers of cloud services, cloud service agents, cloud auditors and carrier. Therefore, once the crime is committed, every participant should assume the corresponding legal responsibility. At the same time, the law should protect their rights. All of these are required to make sure by laws and regulations. For example, Cloud users make use of huge computing power obtained from IaaS, and they commit a crime that violate the information system of financial sector. In this case, it is the lack of supervision or collaborative crime, the cloud service provider and cloud service agents should assume how much legal responsibility to their respective. The relevant laws should make the legal responsibility of five participants clear.

- Improvement of definition and judgment of criminal standard in cloud computing environment

In the "cloud crime and forensics" chapter, this text has analyzed types of crime in cloud computing environment, except for some traditional defined crime, there are some crime that only appear in cloud computing environment., for example "Virtual machine escape" etc. This kind of crime often disguise as legitimate application and engage in data monitoring or illegal attack activity in cloud environment. Another example is the American prism door large-scale monitoring event by Snowden which has raised a babel of criticism in the last two years. In this case, the executants of monitoring act as the subject of crime which get the acquiescence of the cloud computing providers and engage in criminal behavior against the cloud user. The substantive law of our state needs to make certain definition of such new kind of crime and has standard of penalty according to the consequence of the crime committed.

B. Improving or replenishing the relevant procedure law

In china, procedural laws and regulations that can be used in cloud computing environment for enforcement and getting evidence are: 《National security law》, 《law on Guarding State secrets》, 《people's police law》, 《criminal law》, 《Criminal Procedure Law》, 《electronic signature law》, 《computer information system security protection regulations》, 《Internet security protection measures》, 《computer crime scene investigation and inspection rules of electronic evidence》 etc. But given in the special nature of cloud computing, the author suggests that in laws and regulations a few points should be clear:

- Improving the way of digital forensics

With regard to the procedural issues about Judicial Forensic on cloud crimes, 《Computer crime scene investigation and electronic evidence inspection rules》 is the judicial department guidance law used in computer forensics activities in China. The third article in this regulation points out the two ways that the traditional electronic evidence obtained: "on-site inspection" and "remote inspection". "The scene examination" can be used for obtaining evidence in thin client, but "The remote

inspection" shows quite limited effect in handling cloud data in large distributed dynamic virtual machine. Without the help of special hardware and software, "The remote inspection" cannot track and access to the data belong to the same user which may be distributed in a large number of nodes, therefore, add "cloud scene" to the method is on the way.

- Making the conduct and obligations of assisting law enforcement clear

As a new technology, cloud computing is significantly different from C/S, B/S and other previous commercial information service pattern. In C/S, B/S and other traditional business pattern, the server program and data is relatively fixed in position. But in cloud computing's business model, there is no fixed server, program and data are assigned dynamically to computing nodes which are physically presented and distributed. With the calculation of nodes and storage load increase, dynamic transfer may happen in the process. To obtain these distributed dynamic electronic data, get help from the cloud service providers is a must. The sixteenth article of China's "national security law" and the thirty-eighth article of "the law on Guarding State secrets" etc. has clearly defined the information service providers have the responsibility to assist law enforcement evidence. If the cloud service providers with the traditional C/S and B/S operators provide only log, recording events log, however, it will be difficult to obtain the dynamic node virtual machine data. The relevant departments must force the cloud service providers arrange forensics interface in the cloud computing services at all levels (including SaaS, PaaS, IaaS), and when there is necessity, the relevant departments can upload the dynamic node data. China's "Internet security protection technology measures" can make detailed provisions to this, at the same time, we can add "cloud operators must provide digital forensics interface" as a request to the relevant laws.

- Pacific evidence's collection, storage and analysis

《The rules of surveying the crime scene of computer and electronic evidence》in China has for the collection and storage of electronic evidence under the mode of traditional c/s and b/s , but it lacks regulations about electronic evidence's collection, storage under the cloud computing model. Different approaches meet different types of crimes. But in most cases, we have to rely on the access for forensic evidence provided by the cloud service to get the original data , which contains those electronic data needed for electronic evidence that needs to be analyzed. But the large raw electronic data is way too hard to analyze or store. For latest technology, it is common practice to store and analyze through the cloud model itself, but requiring relevant laws, especially 《The rules of surveying the crime scene of computer and electronic evidence》

- The act of law for clear evidence

《The rules of electronic signature》no.7 clarify the act of law of electronic evidence. But it turns out to be a huge problem for the differences in collecting , storing and analyzing etc. Between cloud computing mode and traditional electronic evidence, especially cloud has the traits of multi-users and dynamic. It is exceedingly hard to recreate the crime scene by the evidence from cloud computing mode. Though the evidence from cloud computing is necessary for proving the crime of individual tenants, it needs certain laws like 《Code of criminal procedure》, 《The rules of electronic signature》 and other relevant laws to certainty its desirability and the competency of this kind of evidence.

- Clarifying the procedure or methods for collecting extraterritorial evidence

As for the big problem of extraterritorial forensics , i think we can refer to the methods in article The research about migrating the evidence in cloud computing environment [10]), which talks about using migrating the virtual machine to move extraterritorial program and data to the judicial jurisdiction that the suspect lives in. But the related laws should clarify the availability of migration of data. Data migration technologically equals to duplication only if there must have compute code from could service in the domain.

- Establishing the qualification of forensics personnel

《The rules of surveying the crime scene of computer and electronic evidence》chapter I, article sixth says that the personnel who have the implementation of electronic evidence in computer crime scene and inspection shall have certain qualification and skills. These professionals are currently obtained the qualification of forensic professionals, In Shanghai, Sichuan, Shanxi and other places, many professional offices of computer forensic have been set up. In early days，these forensic examiners who are mostly the computer experts commissioned public security bureau or procuratorate. Cloud computing is a new technology that is widely used, but very complicated. Author recommends that these traditional digital forensic personnel need to carry out the training and assessment of new technologies, and new exams for qualification for new applications are ought to be increased.

V. TECHNICAL ANSWER TO CLOUD FORENSICS DIFFICULTIES

Technically, great challenge of cloud computing technology nowadays are been bringing to the traditional digital forensics, many scholars who are domestic or foreign, new or old scholars, have been studied for it from different angles. At home, Professor Xu Rongsheng in the "security monitoring and forensics" pointed out the difficulties in the security in cloud computer and digital forensic；Wu Gang and Mai Yonghao analyzed the difficulties and solutions about the cloud computer digital forensics; Wu Shaobing carried out the research about the key technology of cloud computing environment of digital forensics [12]; Gong Wei put the theory of cloud computing into computer forensics, and came up a cloud forensics model [13]; Wu Lu designed a cloud computing evidence system [14]; Zhang Jun designed the computer simulation model of a cloud environment [15] ; Xie Yalong, Ding Liping proposed the framework ICFF[16]，the cloud forensics in IaaS mode.

Abroad, John.W.Baghy analyzed certain problems of cloud computing forensic [17]; Keyun. Ruan led the research team to study the digital forensics way, method, steps in cloud environment, and came up to some forensics reference model in Google Apps , WindowsAzure, Amazon S3 and other cloud computing [18]; Josiah Dykstra etc. argued the traditional digital forensic tools technology in the cloud and the related regulation [19].

On the base of research of predecessors, the author puts forward a simple digital forensics model in figure1. The evidence may have two different imputation methods ： center-collection and remote upload. As for the high logic application, such as SaaS, PaaS, IaaS， mostly use information-using central collection method. As for the low logic application such as virtual layer, hardware layer, equipment layer ， use remote upload access to electronic data in order not to destroy its application .The data went through the pretreatment with Hadoop as the platform into evidence storage and to be analyzed by judicial forensic and then the construction of the chain of evidence is been made. After that the evidence will be presented in visual way to judicial institutions.

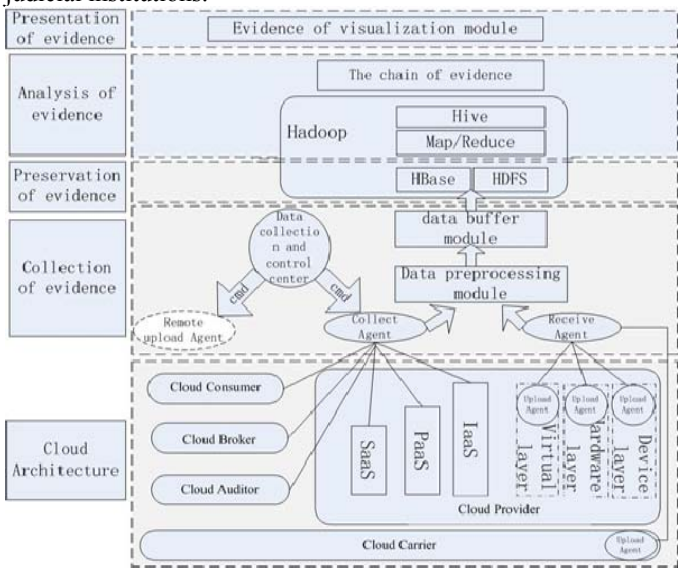

Figure 1. Cloud forensics reference model

VI. CONCLUSION AND PROSPECTS

This paper analyzed the possible types of crimes under the cloud computing environment and combined the characteristics of computing technology to analyze the forensic and technical problems in traditional digital forensic computing environment. Then the paper put forward suggestions and solutions from two aspects that are law and technology, to solve the problem that traditional digital forensics technology cannot always calculate in the cloud. According to what is been mentioned below, future research could be carried out in the respects of regulations refinement and forensics program upgrade and expansion.

ACKNOWLEDGMENT

The corresponding author of this paper is CHEN Hai-Yan. This paper is supported by Projects of the National Social Science Fund (No.06BFX051); Shanghai university training and selection of outstanding young teachers in special research fund (No.hzf05046).

REFERENCES

[1] MELL P, GRANCE T. The NIST Definition of Cloud Computing[R]. National Institute of Standards and Technology, 2011.

[2] Reuben JS. A survey on virtual machine security[R].Helsinki University of Technology, October 2007

[3] DDoS: A Threat You Can't Afford to Ignore, Forrester whitepaper, http://whitepapers.zdnet.com/abstract.aspx?docid=1155831

[4] Wang Ling, Qian Hualin Computer forensics technology and its development trends Journal of Software, 2003,14 (9) :1635-1644.

[5] Liu, F., Tong, J., Mao, J. et al. (2011) 'NIST Cloud Computing Reference Architecture' National Institute of Standards and Technology, Special Publication 500-292

[6] Li Xiaokai. The study on cloud computing [D] computer investigation and collection of evidence problem environment. Beijing: China University of Political Science and Law, 2011

[7] Jia Zhihui, Wang Jun. The standard our country computer forensics legal thinking of [J]..2008 Journal of Sichuan Police College, (02): 22-28.

[8] Wang Keyu [D] research on the problem of applying law extraterritorial evidence. Beijing: China University of Political Science and Law, 2007

[9] China cloud computing security policy and legal working group. Chinese cloud computing security policy and law Blue Book (2012 Edition) [M].

[10] week. Research on technology of [D] field for evidence of the migration in the cloud computing environment. Wuhan: Huazhong University of Science and Technology, 2011

[11] Zhou Gang, Mai ever grand, Cao Qiang, et al. Application of cloud computing on computer forensics technology challenges and Countermeasures of [J]. technology of police.2011, (02): 46-48.

[12] Wu Shaobing. Study on the key technology of electronic evidence forensics [J]. computer science under the cloud computing environment, (S3): 146-149

[13] Gong Wei, Liu Peiyu, Chi Xuezhi, et al. Construction and analysis of [J]. Computer Engineering.2012 cloud forensics model, (11): 20-22.

[14] Wu Lu, Wang Lianhai, Gu Weidong..2012 research on Computer Forensics System Based on the [J]. computer science cloud, (05): 89-91

[15] Zhang Jun, Mai ever grand. Cloud computing environment simulation Computer Forensics Research of [J]. information network security of.2011, (10): 13-15.

[16] Xie Yalong, Ding Liping, Lin Yuqi,.2013 cloud forensics framework [J]. Journal of China Institute of communications such as.ICFF: a IaaS mode, (05): 204-210.

[17] John W. Bagby. On Resolving the Cloud Forensics Conundrum[J]. the Conference on Digital Forensics Security & Law, Richmond Virginia. June 10, 2013

[18] Ruan K., Carthy, J. (2012B) 'Cloud Forensic Maturity Model', Proceedings of the 4th International Conference on Digital Forensics & Cyber Crime, Springer Lecture Notes, October 25-26, Lafayette, Indiana, USA

[19] Josiah Dykstra, Alan T. Sherman. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques[J]. Digital Investigation 9 (2012)S90–S98