Advanced Engineering Forum *Online: 2011-09-09*
ISSN: 2234-991X, Vol. 1, pp 76-80
doi:10.4028/www.scientific.net/AEF.1.76

Study on Forensic Investigation of Network Crime in Cloud Computing Environment

Cheng Yan

Department of computer science and engineering

East China University of Political Science and Law

Keywords: cloud computing, forensic, network crime

Abstract. Cloud computing is Internet-based computing, whereby shared resources, software, and information to computers and other devices on demand. Besides the benefits, it provides a new environment and convenience for network crime, which results difficulties and challenges for forensic investigation. This paper reviews the conception of cloud computing and identifies some key issues of network crime. After analyzing the mechanism and architecture of cloud computing, we propose a forensic model to obtain and fix the criminal evidences. Through investigating from cloud and client aspects, we collect relative log files and communicated data packages, which can succeed to monitor network and store original crime behaviors.

1. Introduction

Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resource[1]. Many international companies, such as Google, Amazon, IBM and Microsoft, have promoted the spread of cloud computing, which can be rapidly provisioned and released with minimal management effort or service provider interaction. Along with benefits of reduced cost, dynamic resource availability, it also brings danger and crime for information security, which results in increasing the difficulties of computer forensic.

Network crime is a new criminal action of information age with the characters of openness, uncertainty, virtualization and etc. The implementation of many crimes may be completed in any country instantaneously at any time, and leave nothing trials in the criminal placement, which brings extraordinary difficulties for the crime detection. The paper looks at the new character and damage of network crime under cloud computing environment, and proposes a forensic model to collect evidences in order to restore the original crime behavior.

2. Conception of clouding computing

What is cloud computing? There is no uniform definition of the conception. In Foster defined cloud as, "A computing paradigm which is a pool of abstracted, virtualized, dynamically scalable, managed, computing, power storage platforms and services for on demand delivery over the Internet" [2]. The clouds can be implemented at Private, Enterprise and External levels. The clouds may also be federated into virtual private clouds [3]. The community clouds may also be formed by joining trustful domains of similar activities together to share computing and data storage resources.

Cloud computing can be considered a new computing paradigm with implications for greater flexibility and availability at lower cost. Because of this, cloud computing has been receiving a good deal of attention lately. The deployment models can be divided into three kinds [4]. First is private cloud, which the infrastructure is managed and owned by the customer and located on-premise. The data is controlled and granted to parties trusts. Public cloud is the second model. In the public cloud, the infrastructure is owned and managed by a cloud service provider (CSP) and is located off-premise. So all data is outside its control and could be granted to untrusted parties. A hybrid cloud composes the advantages of the above clouds and allow to access scalability and cost-effectively without exposing mission-critical applications and data to third-party vulnerabilities.

There widely referenced service models have evolved as follows [5].

(1) Infrastructure as a service (IaaS): is a complete IT infrastructure consumed as a service. Each user, or tenant, accesses a portion of a consolidated pool of federated resources to create and use their own compute infrastructure as needed, when needed, and how needed. The pooled infrastructure may be entirely owned and controlled by one organization (private cloud), may be created by joining and federating private resources with third-party resources (hybrid cloud), or may be entirely provided by a third party (public cloud).

(2) Software as a service (SaaS): is software that is used over a network without downloading it to a local compute environment. The software application is accessed over the internet from a SaaS provider and run in the provider's predefined compute environment. Each user is a tenant in the provider's multi-tenant shared environment. Some customization of the software may be allowed. However, it is uncommon for the user to have much control over the infrastructure compute architecture, location, or service levels provided.

(3) Platform as a Service (PaaS): is a compute environment accessed as needed over a network from a service provider. PaaS is used to develop and run software, as an alternative to designing, building, and installing an in-house development and production environment.

3. Cloud issues for network crime

The cloud is a virtual computing environment which provides applications, platforms and software support as services. The applications are extended over the Internet domain to the CSP which maintains computer systems in clusters [6]. All data stored in the Data Centers (DC) large storage are outside the confines of an organization, its firewall and other security control, which bring with an inherent level of risk.

(1) Data store issue

Usually cloud computing services are delivered by a third party provider. No matter private or public cloud, it uses virtualized intelligent method to manage data around the cloud. Along with benefits of reduced cost, dynamic resource availability, consumption based cost, it also brings new challenges for data security and access control when users outsource sensitive data for sharing on cloud serves. Cloud computing is based on the distributed network and every computer in cloud is regard as a node of network. Cloud nodes will be anonymously accessed by the other nodes on the network to spy on the information if they have no security mechanism. If any node has been attacked, it can be used as a middle tool to control other virtual systems. Especially to the government office, financial office and so on, which put large amount data in private or public cloud, failure of security access rights across multiple domains and failure of electronic and physical transport systems for cloud data and backups can lead to data leakage. For example, Microsoft has demonstrated that the dark side of cloud computing has no silver linings. After a major server outage occurred on its watch in October of 2009, users dependent on the company have just been informed that their personal data and photos "has almost certainly been lost."

(2) Personal privacy issue

The openness, visualization, interactivity, anonymity of network environment makes the general protected measures for private rights losing their capability. The network private rights will be violated in many types including of excessively collecting personal information, illegally getting network personal details, lawlessly using others data, private data disclosure and illegal network trade. The private invasion problems have shown new features besides general characteristics. For the reasons of data encapsulation and public transportation protocols, the data resources in cloud are transparent for some technicians who have the prestige rights. Furthermore some data submitted to cloud are not controlled by end users, and their information are exist even though they have deleted own accounts before.

(3) Computer forensic issue

The network crime activities clues are usually focused on Websites, email box, instant message tools, and mobile phone numbers, bank accounts and so on. The scale of internet is enlarged at the broadcasting types through the cloud services with the propagation channels extending. As a result,

the traditional restricts about criminal areas and tools are broken. The computers and related devices are distributed in larger and larger area e.g. from one province to another one or multi ones, which can enhance the difficulty and time for getting criminal information.

4. Forensic model for network crime

Since cloud computing shared resources, software, and information to computers and other devices on demand, it expands the Internet domain with uncertainties of the data storage and exchanging itself. Network forensic system aims to collect and fix the envidences for the network crime in order to analyze and restore the original crimianl behaviors. It includes many procedures such as data acquiration, data filter, element analysis, forensic analysis and conclusion, among which the data acquiration is the most improtant process of the procedure.

To collect and fix effective crime evidences under cloud computing enviroment, we should first understand the mechanism of cloud computing, which is illustrated in Fig.1.

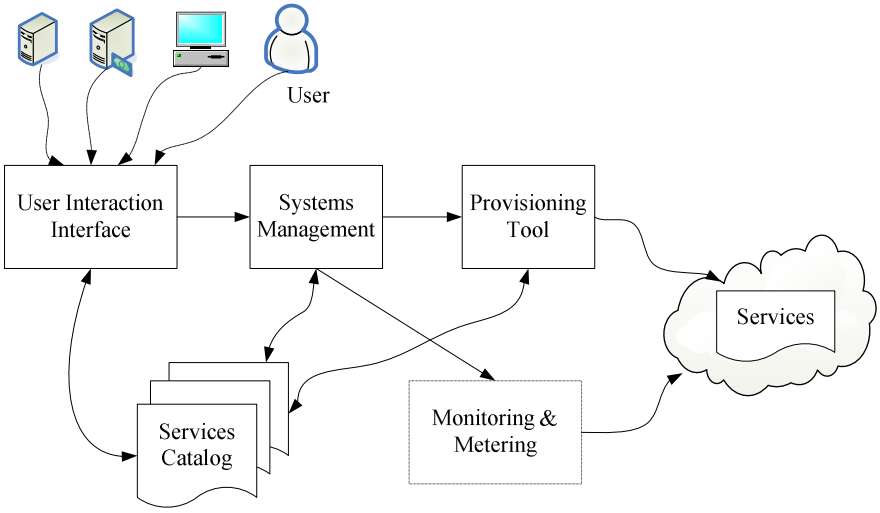

Fig. 1 Basic Cloud Computing Mechanism

As the Fig.1 shown, user interaction interface is based on Web services to access and get user requirements. It allows the user to choose a certain service from the services catalog, which is the list that users can access. After delivering the service requirement to system management to manage and allocate all the resources, cloud services provide tools and environment to carry on the relative programs[7].

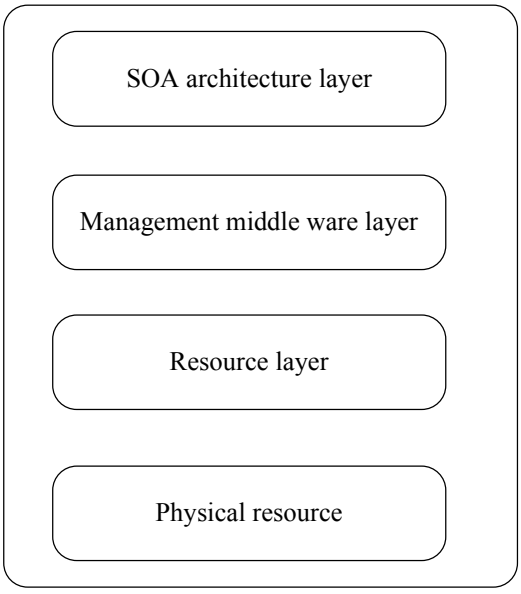

Fig. 2 Basic Cloud Computing Architecture

We abstract the technical architecture shown in Fig.2 and propose a forensic model to collect and fix crime evidences from cloud and client aspects. Fig.3 shows the forensic model for network crime under cloud computing enviroment. Forensic investigation from two aspects as client and cloud can obtain overall envidences. The model aims to monitor network to capture criminal behaviors in real time and collect the relative criminal trials after the event. First, we bulid a database to restore some charactors of criminal behavior. Then we use protocol resolution and intrution analysis technologies to monitor the network. We judge the abnormal data packages through matching them to the criminal behavior database. If analyzing the behavior is crimianl, the relative trasporting packages are restore in the evidence database. Also after the network crime, we collect and fix the criminal evidences from forensic and client aspects in cloud computing enviroment.

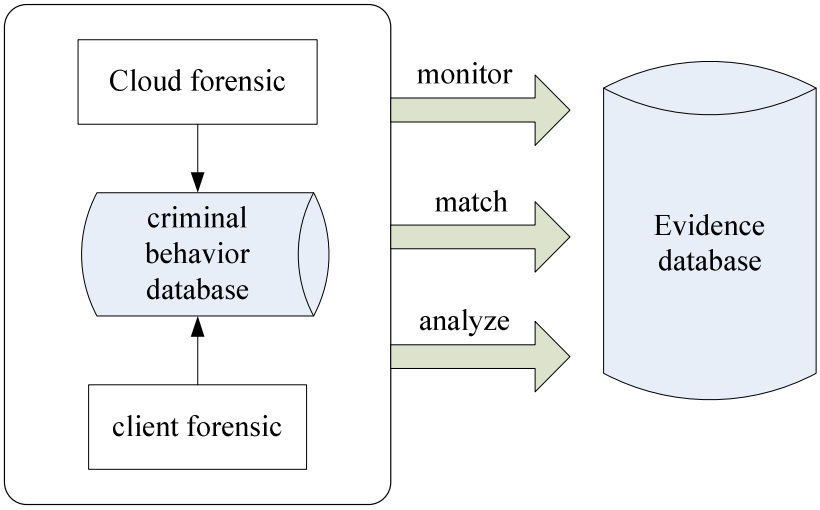

Fig. 3 Forensic model for network crime

(1) Forensic in client

Forensic from client is to get evidences from suspect host in the case. Usually the criminal evidences can be found from serials computer files such as computer log files, electronic files(e.g. MAC time), recovery data, system time, cryptographic file, file slack, erased files,swap files and intrution remain such as program, script, process, IRAM, system buffer cache and so on .

(2) forensic in cloud

Forensic communicated data on the network is regard as the resources of the crime. Sometimes it can obtain some attack evidences easier than that from client host. However forensic in cloud is much difficult than that in client. Since the transmit data packages are dynamic, we use high performance network interface card (NIC) with Libpcap software to acquire data packages. Libpcap set NIC in sophisticated mode and copy packages in core cloud, which are read by network drive programs.

Besides these, some evidences relative to others security products should not be ignored. The log files come from firewall, IDS system, routing, NIC， and others security equipments, etc. Since the cloud computing is supported by CFP, we should collect the resource data based on the different architecture.

5. Conclusion

Network crime is a new criminal action of information age with the character of high technology, security, anonymity and so on. With the development and popularization of cloud computing, the approaches of network crime become more and more mastered and hidden. It has results in the difficulties and challenges investigate in network forensic. This paper focuses on the network forensic in cloud computing environment. The paper firstly gives a brief introduction to the computing conception and then discusses the network crime issues. Based on the architecture of cloud computing, we propose to investigate criminal trials from two aspects as cloud and client. From two aspect to collect trials, we can acquire overall evidences. Usually, the computer log files

electronic files, recovery data and cryptographic files are the key files for our investigation. Besides these, the communicating data package also reveal some criminal trial for us. First, we should bulid a database to restore the charactors of criminal behavior. When monitor the network with the protocol resoltion and intrution analysis technologies, we choose the abnormal data packages and compare them to the above database. If judging the behavior is crimianl, the relative communicating packages are restore in the evidence database.

References

[1] A.Wayne, Jansen, NIST, "Cloud Hooks: Security and Privacy Issues in Cloud Computing", Proceeding of the 44th International Conference on System Science, (2011), 1-10.

[2] Ian Foster, Yong Zhao, Ioan Raicu, Shyong Lu, "Cloud Computing and Grid Computing 360-Degree Compared", Department of Computer Science University of Chicago

[3] Rajkumar Buyya, Chee Shin Yeo, Srikumar Venugopal, "Market-Oriented Clou Computing: Vision, Hype and Reality for Delivering IT services as Computing Utilities" Manjrasoft Pvt Ltd, Melbourne, Australia

[4] T.Rohini, "Comparative Approach to Cloud Security Models", Advances in Computing, Communication and Control, vol.125, (2011), 170-177.

[5] D.Cappelli, A.Moore, R.Trzeciak, T.J.Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition, Version 3, CERT, Jan. (2009).

[6] E.Kowalski, T.Conway, etc., "Insider Threat Study: Illicit Cyber Activity in the Government Sector", Software Engineering Institute, Jan. (2008) http://www.secretservice.gov/ntac/final_government_sector2008_0109.pdf

[7] Chow, Golle, Jakobsson, Masuoka, Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", CCSW'09, November 13, Chicago, Illinois, USA, 2009