The Key Technology of Electronic Evidence Collection Research Based on Cloud Computing

Yanwei XU [1, a], Honghui GONG [2], Ting ZHANG [3]

[1,2,3] Jiangxi Police College, Nanchang 330200, China

[a]xuyanweijx@126.com

Keywords: Electronic Evidence Collection; Electronic Forensic; Cloud Computing

Abstract. A computer system for the new types of objects and tools of criminal activity gradually spread, combat and prevent computer crime has become the public security of the judiciary need to be solved. In this case, the digital forensics have come into being. Digital forensics collected electronic data is often massive and complex sources, different formats, therefore, to a large number of these complex data analysis, this article will cloud computing technology into electronic evidence architecture dynamic, flexible cloud computing platform resources available, the maximum meet forensic requirements. New electronic forensics research methods to explore cloud computing platform is an inevitable trend of development of great significance.

Introduction

Development of computer and Internet technology to bring a great convenience, but everything has two sides, the negative impact of the ensuing greatly filled with people's lives. Computer systems for objects and tools of all kinds of new criminal activities gradually spread, combat and prevent computer crime has become the public security of the judiciary need to be solved. In this case, the digital forensics have come into being [1]. Digital forensics collected electronic data is often massive and complex sources, different formats, therefore, to a large number of these complex data analysis, need an effective way, cloud computing is such a technique, It can analyze vast amounts of data, extract useful information [2].

This paper summarizes the basis of digital forensics research at home and abroad, combined with the digital forensics process, we designed a model of digital forensics and data mining techniques to be applied to the data analysis of the model were. The innovation of this model is that it is in accordance with procedures to design digital forensics, forensics is a comprehensive model, both for stand-alone and network forensics forensics, but also for evidence and after the evidence in a matter of, and in accordance with the specific circumstances requirements, we can take other data analysis techniques. According to the process of digital forensics, the model includes collection platforms, analysis platform and display platform, the article details the functions and composition of each platform, by assuming a security incident may occur, describes the data mining in intrusion detection analysis platform , the suspect locked and audit data analysis.

Related key technology in cloud computing

The concept of cloud computing, there is no uniform standard, which is defined as in the United States, cloud computing is a convenient payment trial mode, in this mode, the need to access structured computing resource pool, fast access to the required resources, and only need to do a small amount of management [3]. This paper argues that cloud computing is driven by the market's large-scale distributed business computing model, and is an Internet based, use and delivery model for the increase of related services. In this mode, the application pool is composed of distributed computers, and all applications are deployed in the shared pool that can be extended by users to use their resources in accordance with the paid use of [4-5].

At present, the types of cloud computing are divided into: public, private cloud, community cloud, hybrid cloud. Public cloud computing platform for public service to the public, providing cloud computing, cloud storage service. Private cloud is a cloud service for internal use, mainly for

individual agencies, through private networks to provide cloud services to the public, the public cannot use these services [6]. The application field of the community cloud services, providing cloud services for a number of Associate Company. The hybrid cloud is the combination of the above two or three clouds. Figure 1 shows the classification of cloud computing.

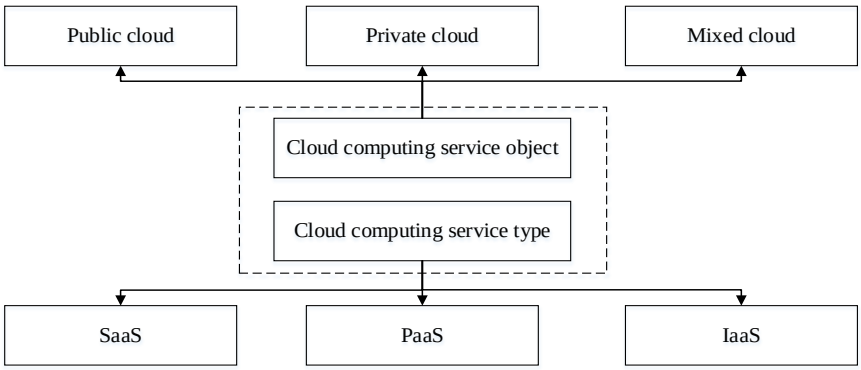

Figure 1.Classification of cloud computing

Cloud computing can provide flexible resources as needed, its expression form is a collection of services. Combined with the application and the current cloud computing research, the architecture can be divided into core service, service management, and user access interface layer 3, such as Figure 2 core service layer, hardware infrastructure, software running environment and application abstract services, these services have very strong reliability, high availability, scalability, meet the needs of diverse applications. Service management is the core business to provide support, to further ensure the reliability, availability and security of core services. User access interface layer to achieve access to the cloud.

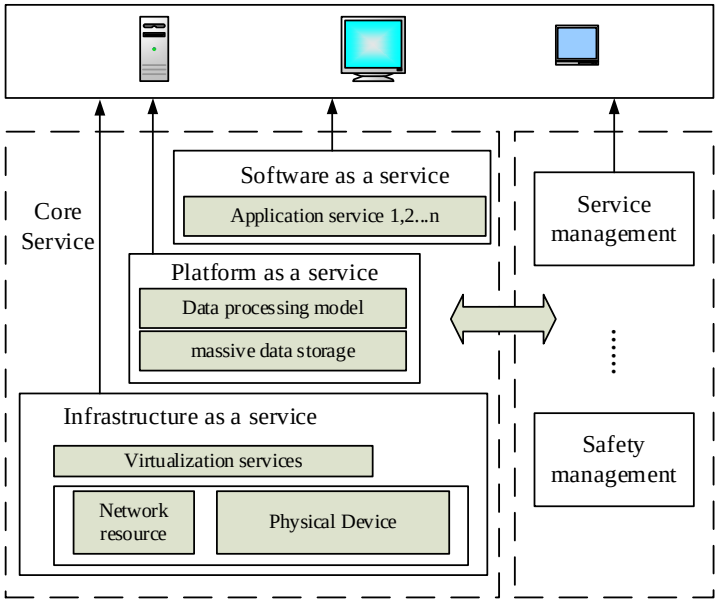

Figure 2.Architecture cloud computing

Analysis Electronic Evidence

Computer forensics generally also referred to as electronic evidence, forensics staff refers to the way in accordance with such laws and regulations, to be able to become recognize legitimate, reliable, credible and there to computers, related peripherals and networks of electronic evidence, acquisition, transport, storage, analysis and presentation of digital evidence process. An important way to get under the traditional method of electronic forensics electronic discovery method is non-traditional crime clues and evidence cloud platform, it is made of electronic evidence

authenticity, legitimacy and relevance is very important, because electronic evidence is convicted of an important basis for sentencing .

With the rapid development of cloud computing, the Internet, networking and other new information technologies, the traditional network topology and resource usage has undergone tremendous change, electronic evidence by conventional methods to obtain electronic evidence are authenticity, reasonable, and effective and other important issues, such as the recovery has been damaged or formatted data with data recovery technology in the cloud computing environment a machine, it will not be complete, true raw data. . At the same time, cloud computing spawned massive data at an exponential rapid growth in the face of such vast amounts of data, on the one hand will lead to evidence of slow problem, on the other hand can not find the evidence will lead to the entry point and other issues. Based on the above electronic evidence under the cloud computing environment include the following difficulties:

a) the amount of electronic evidence of the effectiveness of problem with this issue is decided by the cloud platform itself, the cloud computing platform with resource sharing, resource abstraction and storage distribution, such as direct methods using conventional electronic forensics in the cloud platform On a machine forensics, data will not be complete evidence, because the cloud platform data stored in the form of debris on a completely different machine.

b) the amount of the usefulness of electronic evidence, the depth of the problems of the conventional electronic forensics basic reasoning is weak evidence, to obtain what is what, and cloud platform data large and mixed, if not data processing electronic evidence analysis obtained directly It will be difficult to get useful, in-depth evidence.

c) the development of real-time problem of cloud computing cloud computing era forensics push us into the era of big data, means traditional stand-alone software forensics forensics and electronic evidence can not adapt to the era of massive data, evidence of real-time problem will be cloud computing Another major problem era forensics.

d) evidence of the reliability of cloud computing era problems of the conventional electronic forensics evidence collection process is often no data backup process, so reliability is not high, because once the forensics evidence mistakes led break, will lead to serious consequences.

Electronic forensics based on the cloud computing

In this paper, different from traditional e-discovery technology suitable for new electronic forensics method cloud computing environments. The software forensics technology into a cloud environment electronic forensics process to resolve evidence is incomplete, inadequate and other issues; the next Hadoop architecture Mahout data mining and forensics analysis technology into the process in order to resolve the lack of useful evidence, not enough depth and other issues .Cloud computing environment electronic discovery processes as follows:

(A) to determine the purpose and scope of forensic evidence to determine the objectives and purpose is to grasp the significance of this evidence, to ensure that evidence is obtained in line with authenticity, legitimacy, relevance and thus be adopted by the Court in the proceedings and in cross-examination review stage process be believed, but also to prevent evidence collection process negativity and passivity. Determine the scope of forensic evidence collection process of determining this evidence taken is associated with the case, to avoid taking to electronic evidence irrelevant and a waste of time detection of cases.

(Ii) to determine the source of forensics data due in the cloud computing environment data sources when electronic evidence is evidence from many, have come from large-scale cloud computing data centers, there are data from the cloud service provider, but also from the client's data, evidence objects of different data sources involved are different, forensics target cloud data center is a large cloud storage, cloud service providers forensics object is the relatively small size of the memory and the client object is a forensics the client's memory, cache, files, etc. Earlier determine forensic evidence can narrow the scope of the data sources, to accelerate the pace of forensics purposes.

a) the actual evidence stage in a cloud computing environment using forensics forensics software ensures the reliability of the evidence obtained, completeness and adequacy to avoid traditional electronic forensics forensics defect in a cloud computing environment.

b) evidence of information processing stage due to the cloud computing environment with massive electronic data, which will inevitably lead to a lot of evidence of information obtained evidence phase, which evidence a considerable portion of the information is redundant information, such as the right to process this information , the evidence will not be guaranteed the depth and usefulness. At this stage it proposed using Hadoop architecture Map out to mining and processing of evidence in order to obtain useful information on electronic evidence.

c) evidence evidence Information obtained from the analysis phase step to find the suspects and illegal trace evidence, which is the case a smooth and rapid detection to provide strong support. This paper proposes a new electronic forensic computing platform cloud-based architecture that is "evidence cloud". The forensics cloud hierarchy shown in Figure 3.

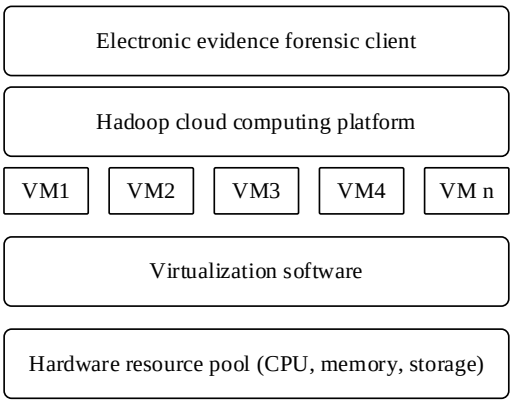

Figure 3.The structure of electronic evidence collection based on cloud computing

The bottom layer of the hardware resource pools, including CPU, memory, storage, network equipment, bandwidth, and other resources, it is evidence of cloud infrastructure layer provides the underlying hardware support; up one for the virtualization software layer, its role is using virtualization software to the underlying hardware resource pool for the virtual machine multiple logical or virtual machine (VM); go down one level to the virtual machine layer, its role with the physical machine, the difference is how resources; the virtual machine layer Hadoop distributed cloud computing platform, which is the core of cloud forensics system that HDFS distributed parallel programming model and memory modules by Map Reduce completed high-speed, real-time, reliable electronic evidence, while after forensics Evidence of redundant information will be cleaned and then provided to the forensic analysis of evidence clearly human data; the last layer of electronic forensics clients, mainly to complete the information collection and display of evidence.

Conclusion

Due to the rapid development of computer technology, computer network crimes are frequent, the traditional way of electronic evidence has been unable to adapt to the current environment, to study new electronic forensic method has positive significance, establish a scientific and rational cloud computing platform electronic discovery system so cloud computing platform It is necessary. Article after a detailed analysis of cloud computing, developed a new electronic forensics method is relatively feasible cloud computing platform, which can be solve related problems, such as when the gathering of evidence does not destroy privacy, evidence in a different cloud computing environments, coping national policies and laws and regulations provide reference.

This article will cloud computing technology into digital forensics problems with network traffic targeting, the background knowledge and background knowledge of digital forensics first cloud computing was an overview is given of network traffic based on digital forensics model of cloud computing, cloud New electronic evidence in the original method of computing platforms

technically carried out reform and innovation, largely make up for the shortcomings of traditional electronic evidence collection methods.

Reference

[1] Dykstra J, Riehl D. Forensic collection of electronic evidence from infrastructure-as-a-service cloud computing[J]. Rich. JL & Tech., 2012, 19: 1.

[2] Taylor M, Haggerty J, Gresty D, et al. Forensic investigation of cloud computing systems[J]. Network Security, 2011, 2011(3): 4-10.

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

[4] Damshenas M, Dehghantanha A, Mahmoud R, et al. Forensics investigation challenges in cloud computing environments[C]//Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on. IEEE, 2012: 190-194.

[5] Dykstra J, Sherman A T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform[J]. Digital Investigation, 2013, 10: S87-S95.

[6] Quick D, Choo K K R. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?[J]. Digital Investigation, 2013, 10(3): 266-277.