Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 13 (15): 2964-2968, 2013
ISSN 1812-5654 / DOI: 10.3923/jas.2013.2964.2968

A Hybrid Cloud Model in the Application of Electronic Evidence

[1,2]Jin Du, [1]Yanhui Du, [1]Ping Zhu, [2]Yu Chen and [2]Yiping Zhang
[1]Chinese People's Public Security University, Beijing, 100038, China
[2]Yunnan Police Officer Academy, Kunming, 650223, China

Abstract: Cloud computing is the most popular Internet computing model currently; its order to solve scientific problems of various information and to provide a powerful technology and resources. In the development of electronic evidence, we combine the characteristics of cloud computing and forensic technology, use the cloud computing method to the electronic forensics and construct a hybrid cloud used for electronic evidence work. In the electronic forensics, based on the combination of information security needs, design a practical forensic model and describes its function and examples. This article complies with actual work needs, compared to traditional methods, introduces new models and features and of successful experiment, for the associated industries and research to provides a valuable reference.

Key words: Hybrid cloud, electronic evidence model, information security, cloud computing

INTRODUCTION

Concept and characteristics of "cloud computing": Cloud Computing is a new technology proposed by Google (2007). It is the product of Grid Computing, Distributed Computing, Parallel Computing, Utility Computing, Network Storage Technologies, Virtualization, Load Balance and other traditional computer technology blending with network technology development and integration (Barroso *et al*., 2003). It is designed a perfect system by the network with a plurality of relatively low-cost computing entities into one powerful computing capability and with SaaS, PaaS, IaaS, MSP and other advanced business model, this powerful distributed computing power to the terminal of users (Armbrust *et al*., 2009). Cloud computing is a core concept of continuous improvement is using the "cloud" of processing power, thereby reducing the processing burden on the user terminal, eventually reduced it to a simple input and output devices and can enjoy on-demand "cloud computing" powerful capability (Krissi, 2010). Renowned consulting firm Gartner defines cloud computing (Mell and Grance, 2009) as "cloud computing is the use of Internet technologies to the large and scalable IT capabilities together as a service to multiple customers technical." The basic principles of cloud computing is distributed computing by making a large number of distributed computers, rather than the local computer or a remote server, enterprise data centers run more like the Internet (Newsroom, 2008). This makes it possible to switch resources to the desired application, based on demand access to the computer and storage systems.

Electronic evidence: Electronic evidence is often called computer evidence. It is the way of electronic evidence identification, acquisition, transmission, storage, analysis and presentation stored in a computer, related equipment and network, in accordance with legal norms, legitimate, reliable, credible process. Electronic evidence is critical files, images and messages generally; sometimes the details of the computer work in the past, such as evidence and other network activity. Including electronic discovery to identify, collect, fixed, extraction, analysis, interpretation, confirmed that the recording and the electronic device described electronic data multiple steps. Electronic discovery process is composed of multiple aspects of technology system. The purpose of electronic evidence is found clues, facts of the case.

Traditional evidence model: Although, China's evidence technology has been developed a few years' time but most domestic evidence is still stuck in the "independent" technical operations stage. The so-called "independent" refers to the use of independent evidence equipment corresponding operation of various stages in the evidence analysis, using artificial way to put the result of previous stage, "enter" to the next stage; leads to inefficiency, numerous processes, no flow of operations. Add to such the human factor error rate increases; in each procedure the physical media or data transmission, media increase the chances of loss or damage.

Based on the above problems, it is necessary to think about and consider the adoption of new technologies to extend or replace the existing evidence system.

Corresponding Author: Jin Du, Chinese People's Public Security University, Beijing, Yunnan Police Officer Academy, China

Compared with the traditional model compared in stand-alone or network applications, cloud computing has very significant characteristics:

- **Data is secure:** Cloud computing offers the most reliable, secure data storage center, users do not have to worry about data loss, virus attacks and other problems
- **Client demand is low:** Cloud computing on the client device requires a minimum, it is also the most convenient to use
- **To share data easily:** Cloud computing can easily achieve data between different devices and application sharing

"Cloud computing' applications in the electronic evidence: In the field of evidence applications, cloud computing architecture is able to bring us:

- Integration of resources, unified and coordinated management of medium access the evidence, the evidence obtained, evidence storage, automated analysis, key recovery, the environment and other functions to reproduce
- It does not limit the client location, as long as a node can access the private network (VPN access or otherwise) can be remotely operated by the security control
- Client requires lowest, without having to install a variety of evidence tools, systems, as long as you can access through IE way to avoid duplicate construction evidence system
- It can be constructed around multiple private clouds or private cloud will all be integrated into "cloud clusters" to achieve resource information sharing, provide limited information query or remote collaboration, remote assistance and the ability to multi-range correlation query and analysis
- High enough in the security permissions under the premise able to remotely control all the cloud computing resources services for one or more tasks, to achieve more than one task, multiplayer multi-tasking, multi-task concurrent per person work
- Most of the traditional evidence mode can be handled through the cloud and unified generate reports, manage storage and distribution
- Corresponds to the cloud within the system nationwide network, in a certain size and resources, you can also provide cloud services. For example, evidence GPS, IM information inquiry, evidence sharing of resources, the key line parsing, email evidence, relational query analysis

EVIDENCE MODEL DESIGN BASED ON CLOUD COMPUTING ENVIRONMENT

Cloud computing environment evidence mostly dynamic information which can be divided into two categories: one is from the local client's dynamic information, including case occurs the client's operating parameters, mainly local client memory information, process conditions, buffer area information, documents to read and write and so on. The

Information is complete chain of evidence at an important part of the client. The other is a cloud computing environment of network traffic, including network communication protocol, packet size and the ability to provide computing resources to the entity location of the ports used, the network connection time and so on. This information is cloud resource provider information. According to the characteristics of cloud computing environments, design evidence model as shown.

In this model, the client terminal each interaction with cloud resources by extracted real-time data acquisition module. Data will enter intrusion detection module, comprehensive testing client terminal with all the interactive information cloud resources. Once a database with intrusion patterns matching information, the module will active the intrusion response module and evidence extraction module. Intrusion response module send alarm information at the same time, it will trigger a response of security control module, thereby protecting the client terminal information security. Meanwhile, intrusion response, alarm and security control information log module is loaded, to prepare for subsequent review analytical purposes and log module can be used as evidence in the evidence base information can be real-time input. Evidence of suspicious information extraction module will be filtered extract evidence preservation module will then extracted data as evidence for data encryption, digital abstract, stamped after the encrypted transmission to the real evidence of the database. Finally, the information generating evidence evidence analysis report submitted to the court in accordance with legal procedures. This model has implemented the cloud computing environment evidence four basic requirements, obtaining evidence while ensuring the integrity of evidence and reliability.

ELECTRONIC EVIDENCE BASED ON HYBRID CLOUD DESIGN

The model is the key and core of the cloud evidence, how to implement the "cloud evidence"? Required the following procedure:

Step 1: To determine the purpose of cloud evidence needs

Step 2: Identify the type of cloud evidence service (PaaS, IaaS, SaaS)

Step 3: To determine the type of technology used in the background

Step 4: For the client: the client to determine the user's role; by evidence tools collected in the implementation of the client's activities

Step 5: For server-side: the presentation of evidence and cloud service providers exchange; collected from a cloud service provider logs; cloud service provider from all the evidence collected

Step 6: For the development side, all collected from the developer evidence; identify the tools used to upload data; determining time consistency of the cloud service provider

In these steps, confirmation is completed; we can build a model based on a hybrid cloud evidence as shown.

Hybrid cloud electronic evidence arranged three main parts: public cloud, private cloud and terminal access. Public cloud refers to public resources, public services, public evidence and publicly available data it comes from a variety of cloud network, the various information collection after processing large data stored in the cloud to provide access to the private cloud use; public cloud supplied to the private cloud data and services required which are open in various related industries can be used; private cloud is stored evidence of the need for confidentiality, rules, user information and intrusion patterns, etc., critical cloud core mainly carries a critical private cloud computing platform processing resources, storage, dispatch centers and certification centers which is the brain of each private cloud which is designed in Fig. 1 evidence model; user terminal can access to the cloud from a variety of clients within the network side component, by a single sign-on mechanism, storing user information in the cloud certification, you can log in at any access point cloud and applications.

How to use such a cloud? In the actual work, we can use it to complete the log monitoring, investigation, data and system recovery, troubleshooting and so on. Electronic evidence functions in the hybrid cloud.

Log monitoring:

- In the cloud computing environment, compliance with laws and regulations, the association between multiple systems with other log entries collaboration and associated data collection, analysis and audit, etc

Investigation:

- For violation of multi-jurisdiction and multi-tenant cloud computing environment investigation
- Suspicious transactions, operations and incident response system cloud investigation
- Cloud event reconstruction
- Provide evidence to the court
- Provide resources and collaboration of law enforcement parties

Data system recovery:

- Recover data, when the data is accidentally or deliberately deleted, modified in the case
- Recover encrypted data, when the encryption key is lost in the case
- Data recovery from accidental damage or system

Compliance with laws and regulations, due diligence:

- Help organizations as required by law exercise of responsibilities to protect sensitive information and maintaining disclosure protected information, making all kinds of reporting instrument, monitor intrusion, constantly updated evidence base, provide evidence of the legitimate call and so on

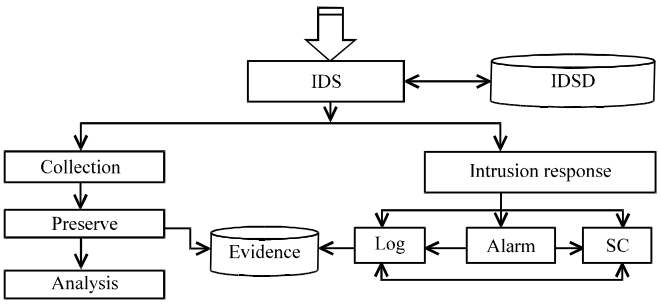

Fig. 1: Evidence model of cloud computing

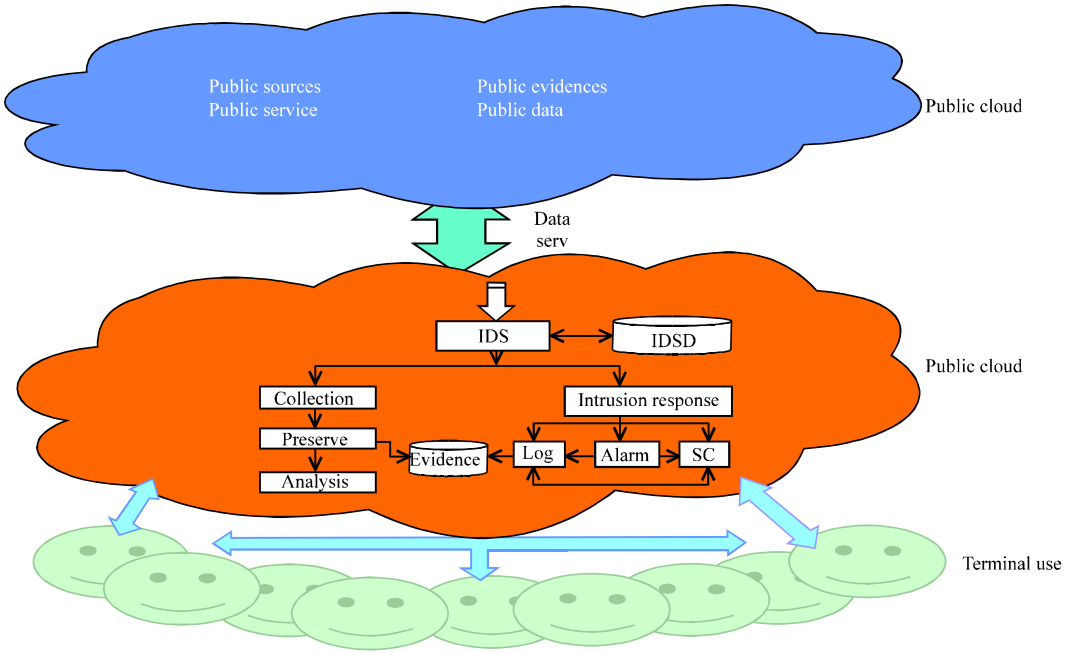

Fig. 2: Electronic evidence based on hybrid cloud

Troubleshooting:

- Locate the data file and to track related modules in a cloud environment
- Determine incident trends over time, across multiple events to identify root causes and develop new strategies to prevent similar incidents from happening again
- In the current state of cloud computing, tracking and evaluation of events
- Solve cloud computing applications and cloud services and other issues
- Solve business problems of cloud systems
- Processing cloud computing environment security incidents

CASE STUDY

Application examples 1: Department of Public Safety established a powerful processing, computing power and storage capacity of the cloud core in provincial-level units. We put the traditional evidence model in these steps: fixation and storage of evidence, search and analysis of evidence logical recovery, system process to reproduce, key recovery and format of report generation and so on, with the electronically integrated into a cloud platform for processing; Certified by the unified dispatch center to coordinate resources within the cloud service evidence tasks; significant savings in labor costs and failure rates. And the dispatch center can also invoked the public cloud resources available, so that the limited capacity of the terminal extended a single cloud computing capabilities, to facilitate resource sharing and remote assistance. At this point, all operations evidence process, query, analysis were scattered in various computing resources, the client need only be sent through IE or other instructions to complete the analysis of evidence analysis work. In such a hybrid cloud, because all resources and services are done in the cloud, for the user, only see an enormous cloud; in one or more resource fails, the system can automatically task distributed to other free resources, will not affect the execution of the task the overall effect of significantly, reducing the error rate and the failure rate. Apart from evidence of the input stage is a human operator, the other steps are process can be automated; evidence efficiency has been improved significantly.

Application example 2: Architecture of this hybrid cloud, we can trace from the behavioral, evidence fixed and recognition aspects to work of evidence analysis:

- **Investigate from the cloud:** In cloud computing, many of our actions can be directly done online. A few large companies can establish a private cloud, public cloud and enterprise cloud, such as Google, IBM, Microsoft and Amazon and so on. Google's private cloud provides online photo storage, editing,

document editing, form editing, etc., we can operate directly on the Web pages without to install a Microsoft OFFICE software client. Therefore evidence surveyed focus to the other end of the network (Web pages). Of Justice Authority under the premise we can directly access from the cloud computing node data Development Company, find a network environment involved in the illegal use of traces and evidence

- **Investigation from the cloud services:** Most companies are small cloud services and modules providers, when some cases not importance or directly, we can investigate evidence from a cloud service provider. For example Alibaba affiliated with at least 50 telemarketing service companies in the investigation, we can directly to identify and search evidence from these enterprises, than the cost of access to data evidence investigation directly from the cloud is much lower
- **Investigation from the local terminal:** Although, a lot of data in the cloud computing are passed across the network but these data will be stored in accordance with the importance of the different cloud environments and the fixed media. During editing, modifying and passing will produce some file fragmentation, web cache left in the local computer that can be focus on evidence obtain such evidence from a local terminal

CONCLUSION

Cloud computing prospects are very bright. However, in the development process, the security challenge is unprecedented bringing to the judiciary. Electronic evidence is a set of evidence science, computer science and behavioral evidence analysis and other disciplines for the integration of multiple interdisciplinary rising in recent years. This study analyzes the characteristics of cloud computing, based on it to design the cloud computing model and hybrid evidence clouds, study their functions, usages, advantages and examples. The author believes that information security is an important aspect of cloud computing research today and with the wide application of cloud computing, electronic evidence will also be a revolutionary change. Therefore, safety technicians and judicial officers should be dedicated to meet this challenge together.

ACKNOWLEDGMENTS

This study was supported by National Natural Science Fund of China (71173199); Science Fund of Yunnan (QN2013055); Science and Technology Fund of Yunnan (Effective management decision-making behavior of the network cluster model Based on public opinion perspective); Research Fund for the Central Universities (2013LGX02).

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph and R.H. Katz *et al*., 2009. Above the clouds: A Berkeley view of cloud computing. EECS Department, University of California, Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Barroso, L.A., J. Dean and U. Holzle, 2003. Web search for a planet: The google cluster architecture. IEEE Micro, 23: 22-28.

Krissi, D., 2010. Distinguishing cloud computing from utility computing. http://www.ebizq.net/blogs/saasweek/2008/03/distinguishing_cloud_computing/

Mell, P. and T. Grance, 2009. Draft nist working definition of cloud computing. National Institute of Standards and Technology. http://www.elasticvapor.com/2009/08/updated-draft-nist-working-definition.html

Newsroom, G., 2008. Gartner says cloud computing will be as influential as e-business. http://www.citeulike.org/user/xeon123/article/10624274