Advanced Science and Technology Letters
Vol.82 (SoftTech 2015), pp.1-5
http://dx.doi.org/10.14257/astl.2015.82.01

Technologies based on Cloud Computing Technology

Huan Ma[1], Gaofeng Shen[2] , Ming Chen[1] and Jianwei Zhang[1]

[1]Software Engineering College, Zhengzhou University of Light Industry,
Zhengzhou 450002, China
[2]School of Computer and Communication Engineering,
Zhengzhou University of Light Industry, Zhengzhou 450002, China
songge19840416@163.com

Abstract. This paper, upon the use of cloud computing resource sharing, storage distribution and other characteristics and based on the analysis of cloud computing environments difficulties on digital forensics, new digital forensics methods and new digital forensics architecture in the cloud-based platform are proposes to meet rapid forensics needs in the era of cloud computing and to deal with the effectiveness, usefulness, depth issues and real-time and reliability problems.

Keywords: Digital forensics; Cloud computing; Forensics architecture.

1 Introduction

In our current digital age, it is startling to see the ease with which digital media can and is being manipulated to alter our sense of reality. Whether it is a Hollywood studio, a national news organization, or an average computer user, the images and sounds that are being created can no longer be unquestionably believed. The courts, in particular, are wholly unprepared to contend with the sophisticated digital technology that allows even the most novice of users to alter our sense of reality[1].

Cloud computing technology revolution gives birth to the era of big data, and how to quickly obtain digital evidence needed in the vast amounts of data has become an important issue for electronic forensics experts to deal with [2-4]. If there is no evidence of an effective framework, forensics cycle will be greatly extended and digital evidence will be damages and destructed, thereby affecting the successful investigation of cases. This paper proposes a new method of digital forensics and forensic measure to solve the problem of evidence under the new cloud computing environment. In this paper, a great cloud computing platform resource sharing and scalable on-demand computing power advantages are made use and cloud computing architecture based on forensic evidence is proposed to solve the problem of timeliness.

2 Cloud computing and digital forensics

ISSN: 2287-1233 ASTL

2.1. Conception of cloud computing

Currently, cloud computing technology is one of the most concerned new computer technologies, often referred to as "cloud"[5]. It is an infrastructure of on-demand delivery resources and charge by using. It makes the goal of computing services clearer, at the same time promoting high efficiency and low cost of such services. Its openness has attracted many developers and researchers, and recognized by the market.

Firstly, we identify cloud forensics as a cross-discipline between cloud computing and digital forensics. There are various definitions for both cloud computing and digital forensics to this date, and in this paper we adopt the current definitions for both cloud computing and digital forensics from NIST: Digital forensics is the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing has five essential characteristics, i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Depending on the division of deployment model, cloud computing has three models: public cloud, private cloud and hybrid cloud, in which hybrid cloud is a special kind of model built up based on private cloud. NIST (National Institute of Standards and Technology) with some of the characteristics of a public cloud authoritative believes that cloud computing can be divided into three levels according to the service form: IAAS, PAAS and SAASO.As shown in Figure 1.

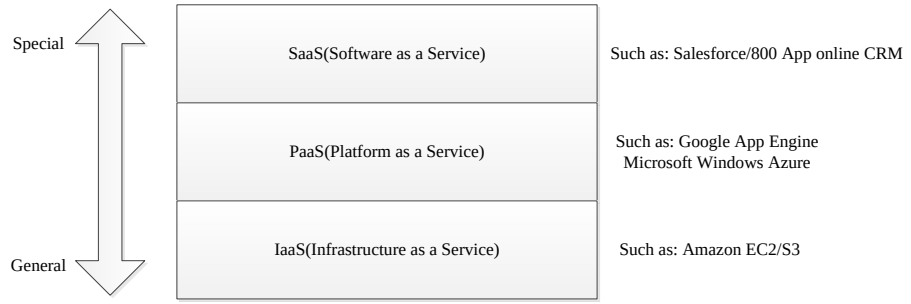

Fig.1. Special to general process

Secondly, we recognize cloud forensics as a subset of network forensics, as network forensics deals with forensic investigations in any kind of public or private networks, and cloud computing is based on broad network access, thus technically, cloud forensics should follow the main phases of network forensic process with extended or novel techniques. The definition of cloud forensics as the application of digital forensics in cloud computing as a subset of network forensics, as shown in Figure 2.

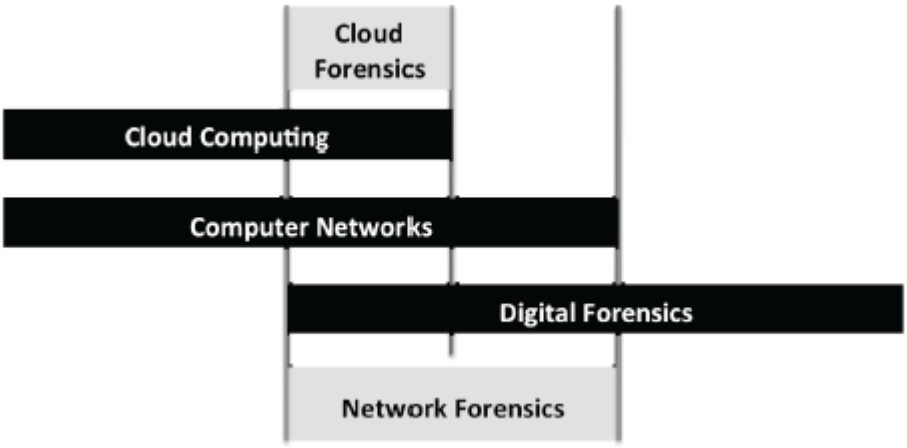

Fig. 2. The definition of digital forensics applied in cloud computing

2.2. Digital forensics

Digital forensics is a branch of forensic disciplines, which includes all of the work process of obtaining evidence from electronic devices and analysis of them. Digital forensics is a relatively new science. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology. Whereas computer forensics is defined as "the collection of techniques and tools used to find evidence in a computer", digital forensics has been defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations".

Digital forensics have been derived from the term of computer forensics, and its oriented object is electronic devices but not just the computer, which is due to law enforcement authorities find in today's environment that people use a variety of electronic devices [6-8]. So the crime is not just computer-related equipment, particularly in the current popularity of intelligent terminals, the source object and criminal offenses are increasing. During the study of digital forensics, many experts has described its concept, but what now widely recognized by everyone, is still DFRWS's definition for digital forensics: "Digital forensics is a process of saving, mobile phones, validation, identification, analysis, interpretation, archiving and reasoning to the data of digital devices with the derived and proven methods, which ultimately facilitates that the investigators reconstruct the chain of evidence and criminal procedure.

Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal

activity, not just computer system. While computer forensics tends to focus on specific methods for extracting evidence from a particular platform, digital forensics must be modeled such that it can encompass all types of digital devices, including future digital technologies. Unfortunately, there does not exists a standard or consistent digital forensic methodology, but rather a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers. Palmer suggests that the evolution of digital forensics has proceeded from ad hoc tools and techniques, rather than from the scientific community, where many of the other traditional forensic sciences have originated. This is problematic because evidence must be obtained using methods that are proven to reliably extract and analyze evidence without bias or modification.

3 Conclusion

Digital forensics is an application-oriented topic, whose research has always revolved the needs of forensic work, so a good performance, high accuracy and stability are the three basic tasks needed attention. Combining cloud computing with digital forensics solves to find a new solution to many questions. The study results of this paper will provide new research methods and research perspective for electronic forensics researchers.

Acknowledgments. The National Natural Science Foundation of China (U1204609); The Education Department of Henan Province Science and Technology Key Project (14A510011); The Youth Science Foundation of Henan Normal University (2012QK21)

References

1. M Reith, G Gunsch. An examination of digital forensic models. International. Journal of Digital Evidence.(2010) .
2. Sue M, Glenda A..Describing records in context in the continuum. The Australian recordkeeping Metadata Schema. (2000).
3. Wen-ping Ma. Efficient without certificate signature scheme based on ID. Journal of communications,(2008), 29 (2). pp: 87-94.
4. Lei Zhang. A class without a certificate of the structure of the signature scheme method. Journal of computers, (2009), 32 (5), pp: 940-945.
5. Fengyin Li, Zhenfang Zhu. Efficient without certificate signature scheme. Computer engineering and application, (2011),47 (10):pp: 23-26.
6. Mark Reim. CalT&Gregg gunsch.an examination of digital forensic models. international journal of digital evidence .(2002)
7. M Reith, G Gunsch. An examination of digital forensic models. International Journal of Digital Evidence (2010).
8. Liles, S., Rogers, M., Hoebich, M. A survey of the legal issues facing digital forensic

experts', Advances in Digital Forensics ,(2009),pp:267-277.
9. Meyers, M., Rogers, M. Computer forensics: The need for standardization and certification. International Journal of Digital Evidence, (2004).3(2)..
10. Beebe, N. Digital forensic research: The good, the bad and the unaddressed. Advances in Digital Forensics .(2009).pp:17-37.

