Study and Realization of Digital Forensics Key Technology Based on Cloud Computing

Bin Zhao
Software Department, Hebei Software Institute, Baoding 071000, China.

Abstract

Rapid development and popularity of the Internet have led to a drastic surge in new-type crimes including illegal computer invasion, severely threatening people’s property safety and information safety. How to control computer crimes and safeguard a healthy Internet environment has become an important issue. As a new technology based on the Internet, cloud computing can provide multiple information services such as computing, storage and application with friendly user experience. Digital forensics by cloud computing has become a new battlefield in the fight against computer crimes and proved effective. The thesis herein explores the concept of digital forensics under cloud computing environment, defines digital forensics key technology of cloud computing and analyzes its realization route after a thorough study on it based on construction of a digital forensics model.

Keywords, Cloud Computing, Digital Forensics, Key Technology, Digital Forensics Model, Realization Route.

1. STUDY BACKGROUND

1.1 Literature Review

In recent years, Internet has become accessible worldwide, leading to a surge in digital computer crimes. Computer crimes such as online money laundering, network attack and information interception increasingly threaten network safety. Computer criminals commit crimes through chat logs, e-mails, webpages and domain names which are necessary for digital forensics technology. Digital forensics technology is an interdisciplinary subject involving science of criminal law, computer science and law (Lu and Liao, 2015). It can investigate and collect evidence of computer crimes which would serve as testimony for legal responsibilities of criminals. In fact, some foreign countries have widely applied digital evidence in juridical practice and regulated digital evidence by law and China has also made improvement on laws and regulations in this regard. Many scholars have conducted abundant study on digital forensics technology, using probability method to quantify and classify digital evidence and studying its feasibility (Yang and Wang, 2015). Some scholars conducted quantification study on standard of digital forensics key technology, grade categories of digital evidence, quantify digital evidence by assigning weight percentage to corresponding grade and study testifying power of digital forensics technology on digital evidence (Yang et al., 2015). Some other scholars built a digital forensics process model based on requirements of digital forensics and identified process and principles of digital forensics (Yang et al., 2015). In a word, with complicated computer environment making computer crimes pervasive, the original system hardware mirroring method finds it hard to meet demands of networked forensics analysis, which stimulates development of networked digital forensics.

1.2 Study Scope

The thesis herein strives to facilitate judicial department in digital forensics so as to more efficiently combat computer crimes and solve low efficiency and difficulties troubling digital forensics under cloud computing environment due to scattering digital evidence. It explains the concept of digital forensics, defines digital forensics key technology, introduces cloud computing and builds a digital forensics model equipped with direct cycle feedback mechanism accordingly. Then, it studies further digital forensics key technology based on cloud computing, analyzes framework of the digital forensics model and explores realization route of digital forensics key technology based on cloud computing.
2. DIGITAL FORENSICS AND ITS KEY TECHNOLOGY

2.1 Digital Forensics

Originating from computer forensics, digital forensics rises with development of computer technology and network technology and has extended its application to all areas related to digital technology. Most remarkably, traditional computer forensics features computer as its study subject and thus is variably defined. For example, in light of event response, some scholars define it as protection, extraction, identification, interpretation and archiving of computer data (He, 2015). Some other scholars define it as scientific inspection, extraction, analysis and assessment of digital evidence obtained in a legal manner (Ding et al., 2015). With development of computer and the Internet, the definition of computer forensics increasingly demands expansion. IPAD and cellphones have become new-type digital devices in forensics investigation. Against this backdrop, expanded computer forensics is gradually referred to as digital forensics. Digital forensics is defined as such a series of activities as collecting, identifying, analyzing, archiving, maintaining and interpreting digital evidence in related digital devices by feasible theories and methods in order to reproduce computer crime process or prevent and stop premeditated and unauthorized destructive behaviors (Zhang, 2015). Digital evidence, closely linked with digital forensics, refers to all data or information kept and recorded in various digital devices and useful for testifying or reproducing computer crime process. The fact that digital evidence is scattered in different types of digital devices leads to low efficiency and difficult coordination in digital forensics, which would negatively impact collection, analysis and identification of digital evidence. Thus, effective solutions are needed in order to better support judicial departments in combating computer crimes (Gao et al., 2016).

2.2 Key Technology

Key technology of digital forensics mainly includes data reproduction technology, information encryption technology, data recovery technology, data interception technology, data deception technology, data signature technology, malicious code technology, data timestamp technology, scanning technology, IP address acquisition technology, IDS forensics technology, honey trap forensics technology, artificial intelligence technology and data mining technology, providing reliable technical support for digital forensics.

3. STUDY ON DIGITAL FORENSICS KEY TECHNOLOGY BASED ON CLOUD COMPUTING

3.1 Introduction to Cloud Computing

Scientific and technological development has boosted development of Internet of things, e-commerce and social network and brought out cloud computing model which allows people to visit shared resources as needed anytime and anywhere through the Internet. The shared resource pool includes many computing facilities, application programs and storage devices, making all kinds of quality information services available to people through cloud computing. Cloud computing tools can analyze storage capability, computing ability and application service capability as needed by users, bringing huge convenience for users and reducing hardware and software cost for them. The following part will construct a digital forensics model under cloud computing environment for further study on digital forensics key technology based on cloud computing.

3.2 Study on Digital Forensics Model

Based on existing computer crimes, digital forensics aims to collect any legal data or information that can testify and reproduce computer crimes and help investigation by generating an evidence report with the data or information. Sound integrity and legal effectiveness of digital evidence require high efficiency, reproducibility, flexibility, sharability, confidentiality and safety in digital forensics process. As a positive feedback cycle mechanism, digital forensics is not a simple linear process but needs cooperative forensics. Cooperative collection and network sharing can foster accuracy and timeliness of digital forensics to make it more efficient and analysis results more objective and accurate. Refer to Figure 1 for schematic diagram of digital forensics.
According to Figure 1, digital forensics consists of five phases, namely forensics preparation, validation and collection of digital evidence, storage and sharing of digital evidence, analysis of digital evidence and archiving of digital evidence (Hu et al., 2015). In the forensic preparation phase, readiness directly influences following collection and analysis of digital evidence and guarantees effectiveness and legality of digital forensics. Forensics preparation mainly includes three aspects. First, analyze computer crime site. Secondly, decide digital forensics plan. Third, protect evidence provider. Design a digital forensics plan based on analysis of computer crime site, protect digital evidence and attack trace left by computer crime with the help of forensics tools and matching and verification of forensics personnel and create favorable conditions for reproducing digital forensics site. In the phase of validation and collection of digital evidence, it’s necessary to predict digital evidence source to raise efficiency of digital forensics and guarantee digital evidence collection is well-targeted so as not to miss optimal collection time. Acquisition manner, time, source, effectiveness assessment and related forensics personnel information should be noted in collection of digital evidence so that forensics personnel can scientifically validate and analyze integrity and accuracy of the digital evidence. In the phase of storage and sharing of digital evidence, forensics personnel need to upload collected digital evidence of one particular computer criminal case to the digital forensics system for analysis, organization and archiving, which can help forensics personnel adjust manners of digital evidence collection, mine new digital evidence and assess its efficiency and relevance. In this way, accuracy of digital evidence can be greatly enhanced. In the phase of digital evidence analysis, forensics personnel need to cooperatively analyze collected digital evidence by using relevance analysis technology, data mining technology and other key technologies, summarize and conclude analysis results and generate a legal digital evidence report accordingly. In the phase of digital evidence archiving, forensics personnel need to maintain digital evidence according to archiving requirements so as to find it when needed in the follow-up inspection.

3.3 Model Framework

Framework of digital forensics model mainly consists of five layers, namely forensics interface layer, evidence analysis layer, cooperative work layer, evidence acquisition layer and data storage layer. Forensics interface layer mainly includes Web and application server, open API and access control with such functions as data transmission, user access, system integration and extension and function coordination. Evidence analysis layer can collect digital evidence by key technologies such as invasion test, data recovery and honey pot net (Jin et al., 2016). Evidence analysis layer, the core layer of the whole digital forensics model, can perform intelligence analysis for collected digital evidence with key technologies such as relevance analysis. Consisting of digital evidence backup system, database and evidence pool, the data storage layer stores and manages digital evidence and regulates and monitors real-time operation of digital forensics personnel. Serving as major collaboration tool of the digital forensics model, cooperative work layer can provide corresponding cooperative tools for evidence acquisition layer and evidence analysis layer to make sure tasks concerning digital evidence go well under its management (Feng et al., 2016). Refer to Figure 2 for frame diagram of digital forensics model based on cloud computing.
4. REALIZATION OF DIGITAL FORENSICS KEY TECHNOLOGY BASED ON CLOUD COMPUTING

4.1 Realization Method

Cloud computing platform can lay a favorable foundation for realization of digital forensics model. Core components in open-source Apache Hadoop including MapReduce parallel processing model, HDFS distributed file system and HBase non-relational database can remarkably enhance efficiency of digital evidence analysis (Jiang et al., 2016). The system framework adopts TestDisk to recover open-source disk data and Network Miner open-source network forensics analysis tool to proactively intercept Wifi and network data packet and analyze PCAP document and network flow rate. What’s more, Ajax dynamic webpage and XMPP protocol are used for Web client development and real-time communication and file transmission of digital evidence respectively (Yang and Zhai, 2017).

4.2 Storage and Sharing of Digital Evidence with Cloud Computing

Cloud storage system capable of digital evidence storage and sharing and constructed by storing redundant data under cloud computing environment can realize safe storage and archiving of digital evidence and reduce its storage and sharing cost. For the purpose of speeding up concurrent data access and transmission, the model stores digital evidence in different DataNode nodes in the form of data block so that users can read stored digital evidence simultaneously from different DataNode nodes and drawbacks of traditional network data storage system can be fixed effectively (Xu et al., 2017). The model uses LATE algorithm to realize deployment of cloud storage tasks, \( PHS = \frac{PUS}{t} < (1-PUS) \), \( T = (1-PUS)/PHS \). In this formula, \( PHS \) represents progress rate of node task, \( PUS \) represents progress score of a task in shard strategy. \( t \) represents passed execution time of a task and \( T \) represents remaining execution time. The process of LATE algorithm is as follows, if \( SMT \) represents whether a task needs replica, \( SDP \) represents execution number of simultaneous replica tasks, execution number of replica tasks of Hadoop system is smaller than \( SDP \). If \( PHS > SMT \), execution continues. If \( PHS < SMT \), execution ends. If more than one task needs calculation by this formula, calculate time needed by these tasks and then arrange them from low to high and finally duplicate the second task whose execution rate is lower than SMT.

4.3 Study of Digital Evidence

Digital forensics model based on cloud computing adopts blocking mechanism to realize concurrent forensics of digital evidence and deploy tasks, which avoids conflicts during cooperative forensics by forensics personnel (Gao et al., 2017). Besides, the system model also applies concurrence control module which guarantees that one
particular digital evidence can only respond to processing demand of one forensics personnel at the same time by using Vector serialization mechanism and Socket communication technology. In this way, overlapped analysis of the same digital evidence by multiple forensics personnel and concurrent conflicts can be avoided, consistency of digital evidence is guaranteed and response time to concurrent users is remarkably reduced.

5. CONCLUSION

To conclude, development of cloud computing technology provides a reliable development approach for digital evidence forensics. Application of digital forensics key technology based on cloud computing can help forensics personnel in digital forensics by digital forensics model so as to guarantee digital forensics work is scientific and accurate and enhance efficiency and cooperation of digital forensics in combating pervasive computer crimes. However, constant development of cloud computing has led to diverse types of computer crimes, so these key technologies alone can’t meet demands of digital forensics, which means higher technological support for digital forensics is in need.

REFERENCES

Gao Y., Fu X., Luo B. (2016). The cloud forensics review, Application Research of computers, 33 (1), 1-6,