Research Article Impact Factor: 4.226 ISSN: 2319-507X
Punam P. Harkut, IJPRET, 2015; Volume 3 (9): 1627-1639 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

DIGITAL FORENSIC ANALYSIS BASED ON MOBILE CLOUD COMPUTING

MS. PUNAM P. HARKUT[*1], DR. H. R. DESHMUKH[2], MR. N. S. BAND[3], MR. A. R. MUNE[3]

1. M.E. Second Year, Dept. of C.S.E., I.B.S.S. COE, Amravati (Maharashtra).
2. Prof & Head, Dept. of C.S.E., I.B.S.S. COE, Amravati (Maharashtra).
3. Asst Prof, Dept. of C.S.E., I.B.S.S. COE, Amravati (Maharashtra).

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Mobile Cloud Computing is widely accepted as a concept that can significantly improve the user experience when accessing mobile services. By removing the limitations of mobile devices with respect to storage and computing capabilities and providing a new level of security by a centralized maintenance of security-critical software for e.g. mobile payment applications, it is expected that it will find broad acceptance on the business as well as consumer side. Research indicates that Mobile Cloud Computing will additionally help to make visions of context services become reality. Digital forensics is a scientific, logical technique and procedure to collect, keep, and analyze digital data and to report the evidence discovered from them. And purposely, we can define it as an investigative technique to examine any kind of behavior using a computer and to prove the fact relation of it based on the data stored in the computer. In our system we are going to introduce a concept called 'Forensic Cloud' to develop a new paradigm in digital forensics and describe some challenges for next generation digital forensic and how our approach based on mobile cloud computing can solve it. To show the feasibility of the introduced concept 'Forensic Cloud', the paper suggests a technology framework for forensic analysis based on mobile cloud.

Keywords: Digital Forensic, Cloud Computing, Mobile Cloud Computing

Corresponding Author: MS. PUNAM P. HARKUT

Access Online On:

www.ijpret.com

How to Cite This Article:

Punam P. Harkut, IJPRET, 2015; Volume 3 (9): 1627-1639

PAPER-QR CODE

INTRODUCTION

Cloud computing has become one of the mobiles hottest topics. Mobile cloud services are mobile applications or services that leverage cloud computing by hosting the primary processing or data storage in the cloud [1]. Moving computing processing and data storage away from mobile devices and into large data centers, mobile cloud enables the users to improve performance, to share data, and to collaborate with others. By these reasons, service providers in the various fields have been developing mobile applications based on cloud computing to assist people in doing his work at anytime and anywhere through mobile phones. There are some well-known applications, such as Google Gmail for iPhone, Mozilla Firefox, Apples MobileMe, and Windows Azure. In addition to these, digital forensics could be one of good examples obtaining benefits of mobile cloud computing, as well. Digital forensics is a scientific, logical technique and procedure to collect, keep, and analyze digital data and to report the evidence discovered from them. And purposely, we can define it as an investigative technique to examine any kind of behavior using a computer and to prove the fact relation of it based on the data stored in the computer. Therefore, for digital forensics, it is required to obtain an image copy of original digital data without damage and to prove that the computer evidence existed in the specific time.

1.1 Motivation

Considering the benefits of mobile cloud computing, the forensic service based on mobile cloud computing could be good solution to the problems today's forensic tools are facing. In this system, well introduce a service concept called Forensic Cloud to develop new paradigm in digital forensics. And then, our work in progress will be described by presenting the architecture and a service scenario as a kind of mobile computing service.

Existing digital forensic tools have been developed to offer a set of basic features for digital forensics such as evidence imaging, analysis, retrieval and reporting. By focusing on these features, the tools have been upgraded to support for evidence from new media, operation systems and file types. Most forensic tools are available in an integrated tool operated on a single platform OS such as Windows or runs within the media stored on portable hard disk drives for mobility. To improve the processing speed of the tools, special purpose hardware devices also are produced.

For general forensics tools, imaging of 2TB data takes 7 hours. Bit wise search is being processed at a rate of 20MB/s and the search on 1TB forensic image data takes about 14 hours [2]. And a special device is needed to move the confiscated desktop to the forensics lab. The

single platform based forensic tool also has drawbacks in analyzing increasing number of digital evidence. Meanwhile, cloud computing provides the characteristics of rapid elasticity, measured service, on demand self-service, ubiquitous network access and resource pooling. To deal with these limits of existing forensic tools, advantages and characteristics of cloud computing can be used to design an advanced forensic tool. Therefore, we propose the structure and framework of digital forensic software as a service (DFSaaS) for digital forensics procedures on cloud computing, and present the use scenarios of DFSaaS.

Digital forensics is a process to find legal evidence from computers and digital storage media. There are a number of commercial and open source tools for digital forensics investigation. Although typical forensic tools include a lot of functions for examining data on the media such like Windows registry reviewing, password cracking, and keyword searching, today's tools running on a single system have limitation on forensic investigation because they need extremely long time and computational power to analyze the growing size of digital devices. Additionally, the proliferation of operating systems and file formats causes another problem by dramatically increasing the complexity of data exploitation and the cost of tool development.

1.2 Problem Statement & Objective

Nowadays, digital storage of computer data is moving toward cloud computing which is a set of infrastructure provides data storage for organizations and individuals. Due to this large scale, in case an attack occurs in the network of a cloud it would be a big challenge to investigate the cloud. Therefore, digital forensics in cloud computing is a new discipline related to the increasing use of computers, networks and digital storage devices in numerous criminal activities in both traditional and Hi-Tech.

Considering the benefits of mobile cloud computing, the forensic service based on mobile cloud computing could be good solution to the problems today's forensic tools are facing and following requirements should be met.

- High speed processing of basic forensic functions.
- Intuitive presentation.
- Supporting user mobility and secure data access.

Objective of Project

- Fast Analysis

- Supporting various devices
- Pervasive and Collaborative analysis

2.1 Background

Mobile cloud computing is an emerging cloud service model following the trend to extend the cloud to the edge of networks. It includes numerous mobile devices that are closely associate with their users. They will be directly involved in many cloud activities that extend the cloud boundaries into the entire cyber physical system. As predicted by Gartner, mobile phones will overtake PCs as the most common Web access devices worldwide by 2013. Thus, mobile devices will become more important and will be involved in almost all aspects of our daily life. Mobile computing research is to study how portable devices sense and learn the status of devices and the context related to their mobility and networking in order to better support mobile applications in an ad hoc communication environment. Cloud computing research mainly focuses on how to manage computing, storage, and communication resources that are shared by multiple users in a virtualized and isolated environment. Mobile cloud computing cannot be simply illustrated as merging mobile computing and cloud computing technologies.

2.2 RELATED WORK

2.2.1 Mobile Cloud Computing

According to the latest research from Juniper Research, the market for cloud based mobile applications is expected to grow 88 percent annually and reach 9.5 billion dollars by 2014[3]. The number of mobile cloud applications available today is relatively small in relation to all mobile application, but the numbers and their types are growing. According to ABI Research, there are five primary categories for the majority of successful mobile cloud applications while the possibilities of mobile cloud applications are endless. The categories are productivity, utilities, social networking, games, and search [4].

Among these categories, the vast majority of applications in productivity category comprises enterprise-related including data sharing/collaboration, customer relationship management, calendaring/scheduling invoicing/merchant services, multi-tasking, practice management and so on. Today's many mobile applications in this category are part of large cloud computing offerings from companies such as Force.com, Oracle, and IBM. One of the challenges for mobile applications is the inability for users to work within multiple applications at the same time including read-only applications such as news web sites, and Yahoo contributed in this field by

presenting mobile multi-tasking with its new mobile homepage and aggregating services on one page containing news, e-mail, and status updates from several social network sites.

Meanwhile, search is primary capability and necessity for the mobile internet in general. There is a case study for cloud-based mobile search [5].There is another work which discusses the benefits and drawbacks of mobile desktop search coupled with cloud-assisted operations [6].

Digital forensics using mobile cloud could be categorized in productivity area by sharing data and collaborating on a work with others. With an aim to improve efficiency in investigation, digital forensics using mobile cloud enables examiners to access the evidence data stored in the cloud and to analyze them in real-time. In the following section, we discuss the benefits of digital forensics on mobile cloud computing in detail.

2.2.2 Digital Forensic on Mobile Cloud Computing

Today's digital forensic tools have been developed to provide investigators basic functions for digital media examination; they include disk imaging, data analysis and search, reporting and so on. While maintaining those functions, the tools have been upgraded by adding some features needed for handling new physical devices, different operating systems, and various kinds of file types. In the aspect of configuration, most of forensic tools are functionally integrated on a single system of Widows OS. Some tools supporting mobility are saved in the portable memory or portable hard disk drive and runs inside them. Also hardware tools provide exclusive services, such like password cracking, to improve processing performance. These approaches make the forensic tools just evaluated as how many functions they have, what diversity of devices and software they support, and whether they are stable and reliable or not. However, recent researches have suggested new requirements today's forensic tools have to meet as the result of advances and fundamental changes in the computer industry [7][2]. From now on, we describe some challenges for next generation digital forensics and how our approach based on mobile cloud computing can solve it.

Fast Analysis: It needs to improve absolute and relative speed for data examination as digital data has been tremendously increasing. Current indexing speed is about 3.4 MB/s and it is decreasing as data to be analyzed is increasing. In the field of digital forensic analysis, there have been a few studies to break the performance wall. V. Roussev et al proposed a design based on distributed processing and an open protocol for bitwise search [8], J. Lee et al suggested a high-speed forensic search engine using a content processor [9].Scalable architecture of cloud computing gives benefits in improving its performance, and parallel computing on distributed environment provides powerful processing for mobile analysis.

Supporting various devices: As operating systems and file formats are continuously changing, the cost of tool development and maintenance is highly increasing. It is important for digital forensics to examine all files in various formats on the disk and it should handle operating system and file system of each device as well. For example, considering a case of smart phone alone, there are currently five platforms with a market share of 5 percent or greater. It significantly adds development and maintenance costs. These costs are largely obviated by the adoption of the cloud-based service model.

Pervasive analysis and collaborative analysis: Many investigators use multiple devices work PCs, work mobiles, personal computers, or notebooks. Each of which most likely runs on different operating systems and contains specific data and content. This makes it difficult for the investigators to easily access or share evidence data across devices or to maintain unified data. Under the cloud-based approach, as all of the data pertaining to the app is stored in the cloud, productivity in forensic investigation can be improved by co-operating with other examiners and by sharing the evidence. Mobile forensic analysis based on cloud computing enables collaborative investigation to be available anytime at any place.

3. METHODOLOGY

We have been developing a forensic service concept called Forensic cloud to drive new paradigm in digital forensics and studying a technology framework for Forensic cloud [10]. At the same time, we have been developing a mobile forensic analysis application as an example of forensic cloud service to show the feasibility of forensic cloud. Forensic Cloud: The technological and legal environments around digital forensics investigation have been rapidly changing and today's digital forensic tools have some problems in systemically responding the challenges. Therefore we propose new concept called Forensic Cloud to develop new paradigm in digital forensics. The aim of forensic cloud is to enable forensic examiners to concentrate on the investigational process by separating technology from investigation. In other words, it is to make the examiners obtain useful and effective information without subsidiary knowledge for forensic tool operations and management, as providing forensics techniques as services.

- In order to implement this concept, following requirement should be met. High-speed processing of basic forensic functions suchlike imaging, analyzing and searching, password cracking, and so on
- Intuitive presentation
- Supporting user mobility and secure data access

It could be possible by developing forensic service framework based on cloud computing, providing data visualization based on behavior based analysis and correlative analysis, and supporting mobile based forensic environment. We have been developing the technological framework for forensic cloud continuously and implementing mobile forensic analysis at one time.

3.1 DESIGN

3.1.1 Framework Design

In this section, we present the technology framework to implement mobile forensic analysis based on cloud computing. Among various forensic analysis methods, we are particularly interested in forensic index-based search application because it takes pretty long time to construct an index database before searching though it returns response to a query in a short time after indexing. Fig. 1 shows the entire framework for forensic index based search on the mobile cloud computing. The framework consists of 4 layers, which are client layer, front-end layer, data processing layer, and platform layer. The platform layer which lies on the bottom of framework consists of distributed systems. In particular, Apache Hadoop is installed on these systems to manage the distributed systems. Hadoop provides various kinds of features for reliable, scalable, distributed computing [11]. When an application is developed on Hadoop, it can be easily migrated onto other Hadoop systems on cloud. For instance, it is possible to run Hadoop on Amazon EC2 and S3. Amazon has released Amazon Elastic MapReduce services since April, 2009. Therefore, our application based on Hadoop can run on that service without any modification. The data processing layer includes a lot of modules for developing forensic analysis application. There are an Ngram tokenizer and a pattern analyzer for generating index token. A file filtering module is used to extract plain text from various file format such as PDF, MS-Office, Zip files and so on. Additionally, VFS (Virtual File System) library is requisite to mount and handle forensic images which are acquired by the process where the entire drive contents are imaged to a file and checksum values are calculated to verify the integrity of the image file. The inverted index is an index data structure storing a mapping like words, hits, and locations in a database file, or in a set of documents. It is a key part of index search to generate and traverse the inverted index structure. In particular, the inverted indexing module supporting distributed computing is required to provide fast full text searches on massive data.

Full text searches on massive data. Also, it needs to offer the security solutions, such as user authentication and access control because security might be a serious concern over digital forensic analysis on mobile device. In addition, other modules for exceptions handling and

system maintenance are requisite to provide reliable distributed computation. Several servers could exist on the front-end layer to support various kinds of client applications. A server waits for the requests from clients and responds with the results in the suitable form for each client. There are three types of clients on the client layer: Windows application for the lab analysis, web application for the remote analysis, and mobile application for the pervasive analysis.

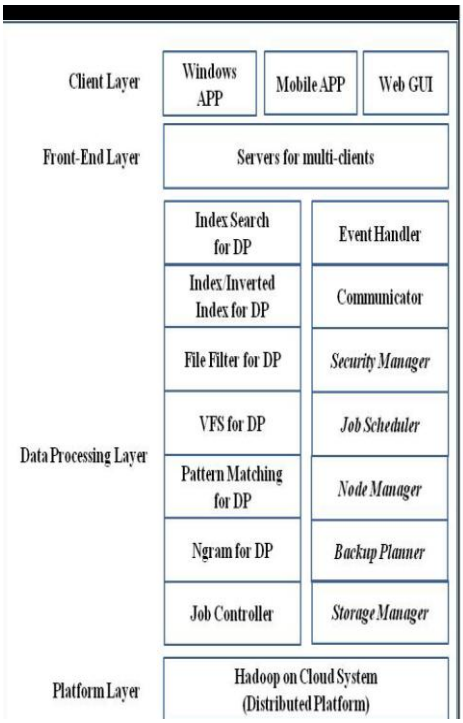

Figure 3.1: Framework for forensic index search on cloud computing.

Data Abstraction for Mobile Device: The general graphic user interface of the forensic search applications consists of several viewers for a directory tree, file contents, a searched list and so on. Although each viewer is used to provide a lot of information for the forensic investigation, adopting these viewers to the mobile application are not suitable without any modification because the display panel of mobile device is relatively smaller than that of the personal computer. Additionally, they have a trouble in intuitionally presenting the searched result. As existing forensic search application just lists the results without a kind of grouping or inappropriate filtering, an investigator has to spend a lot of time in order to find documents related to an investigation among the searched results [12] [13]. Therefore, it is important for the forensic analysis on mobile devices to present searched result well and effectively. There have been several researches to improve human comprehension during forensic investigation,

and D. Ayers discussed, in his paper, that presenting data at higher levels of abstraction than _le system objects can make users productivity and understanding better [7].

In order to solve this problem, we present the data abstraction method for mobile application. Our proposal for data abstraction focuses on the relationship of the data artifacts such as documents, emails, phone numbers, and so on. Fig. 2 is an example for data abstraction schema. A phone number, 010-123-4567, searched by index engine can be found several documents: A.doc, B.xls, C.html. By analyzing file attributes of these documents, additional files, C.html, D.html, E.eml, having same file access time can be reviewed. Besides, other phone numbers and email addresses in the same file with the phone number can be presented to the investigator. These data help the investigator to identify relevant evidence whenever he doesn't have enough ability to recognize and analyze certain types of relevant evidence. This approach might be more effective for forensic analysis on mobile devices, as well. Digital Evidence in Cloud Computing Environment: The evidences are everywhere even if we want to deny it. In scientific angle, the evidence can be our fingerprint, DNA, human witnesses, CCTV, the residue of gun explosion, tools used, alibis, and also cloud computing environment. As in the law, the enforcers have a warrant to be used to enter and search premises, this also applies if the constable required information stored in the electronic form where it includes that the electronic devices are with the suspect such as a laptop, mobile phone, compact disc or external hard disk and the devices is on the property as amended by the Criminal Justice and Police Act. Other than that is the evidence from other jurisdictions such as answering questions or producing articles and information where it also include evidence in digital format. In seizing evidence, for example enforcers enter a premise to inspect and search the premises, if they found that the computers inside the premises are connected and on-line to a cloud storage server, that server is considered as a part of the computer hardware even if the server is out of the country. Thus, the enforcer or investigator may copy the data and information on to the computer of the suspects or they can have the remote access to the server thus they can download the data to any other computer they wish for.

3.2 Model

Apache Hadoop provides HDFS (Hadoop Distributed File System) and Map/Reduce framework. HDFS is a distributed file system that provides high throughput access to application data. The MapReduce is a kind of programming model to develop the distributed computing application [14]. MapReduce programs consist of Map and Reduce module and they are contained in a java jar file with an XML file containing serialized program configuration options. Running a MapReduce job places these files into the HDFS and notifies TaskTrackers, which is running for

work on slave node, where to retrieve the relevant program code. All program is equivalent, therefore, it accesses whatever data is local to a particular node in HDFS [11].

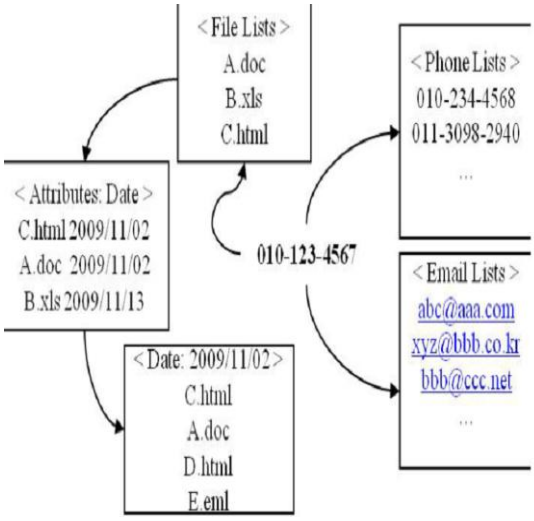

Figure 3.2: Data abstraction of the forensic data

We have designed the index engine as a MapReduce application running on Hadoop and the search engine querying to the index database. When the mobile client sends the indexing request to the server on the master node, the server accepts it and makes MapReduce applications run indexing jobs on the slave nodes. The inverted index created is stored on the HBase and the search process is executed by querying the HBase. This process shown can be regarded as a kind of mobile cloud computing which is carrying out data processing and storing outside mobile devices. The mobile device is simply to be a terminal in cloud computing and intended as a convenient way of accessing forensic services in the cloud.

The Hadoop Distributed File System (HDFS) is a distributed file system designed to run on commodity hardware. It has many similarities with existing distributed file systems. However, the differences from other distributed file systems are significant. HDFS is highly fault-tolerant and is designed to be deployed on low-cost hardware. HDFS provides high throughput access to application data and is suitable for applications that have large data sets. HDFS relaxes a few POSIX requirements to enable streaming access to file system data.

An example scenario of mobile client is depicted in Fig 3.3. Each case of investigation might be downloaded on a mobile device such like general mobile apps to be done. Then an examiner clicks a case and searches what he's looking for. By moving one case onto another case, two cases can be merged and correlative analysis of merged cases is possible. This scenario is very

simple and intuitive for users place, but it needs complex and time-consuming processes. Our mobile forensic analysis makes it possible by moving heavy operations into servers on cloud.

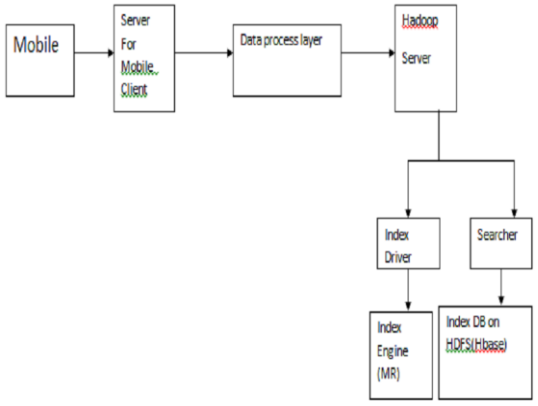

Figure 3.3: Process of distributed indexing and searching

4. APPLICATION

Digital forensics is a branch of forensic science concerned with the use of digital information (produced, stored and transmitted by computers) as source of evidence in investigations and legal proceedings.

Mobile cloud computing brings a lot of opportunities to digital forensics investigators as well as network operators, application developers, and service providers. By using mobile cloud computing, the digital forensic tools can increase the productivity and efficiency in investigation process.

5. CONCLUSION

Developing cloud computing platforms and mobile software in parallel is an intriguing prospect. Existing digital forensic tools operate on a single platform such as Windows OS or Linux OS, which have been constantly improved in processing speed and supporting various media. Recently, the number of evidences in digital media is increasing and to process these data, high speed processing is needed. Enormous digital evidence will require more much processing time and resources to process them. However, a single platform based tool cannot satisfy this requirement.

In this project a forensic service concept called forensic cloud is proposed which drives new idea in digital forensics and studied a technology framework for Forensic cloud to deal with

these limits of existing tools, and associated with mobile cloud computing can help solve these drawbacks.

10. REFERENCS

1. A. Klein, C. Mannweiler, J. Schneider, and H. Schotten, \Access schemes for mobile cloud computing," Intl. Conf. on Mobile Data Management, pp. 387{392, 2010.

2. S. Gar_nkel, \Digital forensics research: The next 10 years," Digital Investigation, 2010.

3. Monetising enterprise consumer market," Juniper Research Mobile Cloud Applications and Services, 2010.

4. Next-generation browsers and widget and sim and network-as-a-service and platform- as-a-service," ABI Research Mobile Cloud Computing, 2009.

5. Y. Gao, L. Fu, Z. Zhang, S. Luo, and P. Lu, \A case for cloud-based mobile search," ZTE Communications, vol. 1, 2011.

6. E. Lagerspetz and S. Tarkoma, \Mobile search and the cloud: The benefits of offloading," IEEE International Conference on Pervasive Computing and Communications Workshops, 2011.

7. D. Ayers, \A second generation computer forensic analysis system," The Proceedings of the Ninth Annual DFRWS Conference, vol. 6, pp. 34{42, sept 2009.

8. V. Roussev and G. Richard, \Breaking the performance wall: The cases for distributed digital forensics," Proceedings of the Digital Forensics Research Workshop, pp. 1{16, 2004.

9. J. Lee, S. Un, and D. Hong, \High-speed search using tarari content processor in digital forensics," Digital. Investing. 2008.

10. D. Hong and J. Lee, \New paradigm of digital forensics: forensic cloud," The Workshop on Digital Forensics, 2010.

11. Hadoop distributed file system," http://hadoop.apache.org.pdf.

12. N. Beebe and J. Clark, \Digital forensic text string searching: improving information retrieval effectiveness by thematically clustering search results," Digital Investigation, pp. 49{54, 2007.

13. B. NL and D. G., \A new process model for text string searching," Research advances in digital forensics III Norwell: Springer, pp. 73{85, 2007.

14. J. Dean and S. Ghemawat, Mapreduce: Simplified data processing on large clusters," 6th Symp. On Operating System Design and Implementation and San Francisco, pp. 137{150, 2004.