IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems
ICIIECS'15

Design and Implementation of Cloud Based Mobile Forensic Tool

Prashant N. Ninawe
Department of Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur, India 441110
ninaweprashant@gmail.com

Shrikant B. Ardhapurkar
Department of Computer Technology
Yeshwantrao Chavan College of Engineering
Nagpur, India 441110
shrikant.999@gmail.com

Abstract— **In order to solve the problem of actively adapt to the desktop application of the mobile forensic tool, a cloud based mobile forensic tool is proposed in this paper. Cloud based mobile forensic tool can largely advantageous from cloud based models in terms of the low cost utilization and better resource management. The purpose of the system design is accounting to retrieve smartphone contents in forensically sound ways by using cloud service models in order to reduce the cost of mobile forensic tool. The data stored on the smartphone could be extremely useful for analysis through the course of an investigation. Indeed, mobile devices are already showing themselves to have a larger volume of probative information that is linked to an individual with just basic call history, contacts and text message data; smartphone contains even mobile useful information such as email, browser history and chat logs. Mobile devices probably have more probative information that can be linked to an individual per byte examined than most computers and this data is harder to acquire in a forensically proper fashion in cloud computing. By comparing this scheme with conventional design schema this system can easy and ubiquitous access to a mobile forensic tool in the cloud, and allow to utilize the services of forensic examiners who may be in geographically remote areas. Therefore, developing a cloud based mobile forensic tool system plays an important role.**

***Index Terms*— Mobile forensic, digital forensic, cyber investigation, cloud computing, cloud forensic.**

I. INTRODUCTION

Mobile forensic is defined as the science of recovering digital evidence from a mobile under forensically sound conditions using accepted methods [1]. The whole process is broadly divided into following four stages: preservation, acquisition, examination and reporting. The preservation is a very first step in digital evidence recovery and it is the process or method of seizing and securing suspect property without altering the content of data that is present in the devices. Acquisition is the process that is coming after data preservation. It is a process of imaging or otherwise obtaining information from a digital device and its peripheral equipment and media. Third step is the examination and analysis, it involves applying tools to uncover digital evidence, including that which may be hidden or obscured. The final and very important step in forensic is reporting. Reporting is the process of preparing a detailed summary of all the actions taken and conclusion suppose to be reached in the investigation of the case. Reporting depends on properly maintaining a careful record of all action and observation describing the result of test and examination.

A. Data Preservation: The very first step in the mobile forensic is the data preservation step in digital evidence recovery and it is a process of seizing and securing suspected evidence or property without deleting or modifying the actual contents that is present in the mobile device or other digital evidences.

B. Data Acquisition: After doing successful preservation of the data the second step of the mobile forensic is the data acquisition. It is the process or method of imaging or otherwise obtaining information from digital evidence and its peripheral equipment and media. There are four types of data acquisition methods are available, they are as follows: Manual Acquisition, Logical Acquisition, Physical Acquisition and Chip-off [2]. All these methods are used for acquiring the internal and external memory data from a mobile phone.

C. Data Examination: Data examination is the process or method of applying tools to uncover or acquire digital evidence, including that which may be hidden, deleted or obscured.

D. Reporting: This stage is most important in digital forensic. Everything done during the mobile forensic is useless if the evidence is not admitted correctly in the court of law to prove or defend the possible crime. The authenticity and integrity of evidence must ensure by a well documented regarding of possessing the evidence from the start of the forensic process to the end of the process when all evidences admitted in the court of law.

II. CLOUD COMPUTING

The word cloud is popular in IT. What is Cloud Computing? Although there are number formal definitions proposed by both industry and academic researchers. For example,

- According to NIST "Cloud Computing is a system for enabling convenient, on-demand network access to a shared pool of computing resources which is rapidly provisioned and released with minimal management effort or service provider interaction." [3]

- According to IBM "Cloud Computing, often referred to as simply 'the Cloud', is the delivery of on-demand computing resources everything from application to the data centers over the network." [4]

- According to Oracle "Cloud Computing is a advancement in the technology which servers information technology and services. By applying on-demand access to a shared pool of resources in a self-service, dynamically scaled manner, cloud computing provides compelling significance in cost, speed, efficiency and reliability." [5]

Mobile forensic tool using a cloud computing strategy, will cost less and greater efficiency. The forensic examiners can maximize the use of the advantages of cloud computing. Cloud resources such as services, processes and applications can be rapidly deployed, thousands of virtual machines in a cloud can be easily managed, and the servers' required power costs can be reduced. The forensic examiner will use less time for analysis of the smartphones. Cloud based mobile forensic tool can obtain services from the cloud including Infrastructure as a Service (IaaS) and Software as a Service (SaaS).

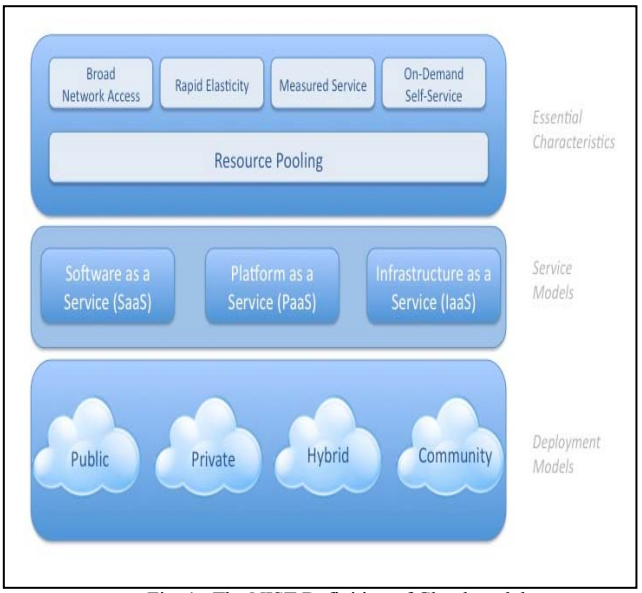

Fig. 1. The NIST Definition of Cloud model.

I.

III. PROPOSED SYSTEM

In the past, mobile forensic investigation teams had to come to the crime scene. Since the crime happens in one city and the cyber forensic lab is in another city, then the main disadvantage is that the mobile forensic examiner has to come to the crime scene. Since it takes lots of time and money. So, with the increased in the use of personal computers, laptops and modern Information Technology devices in mobile forensic, there is an easy way to investigate the mobile device which is based on cloud. But nowadays outsourcing of cloud computing leads to complex system where the mobile phone can be investigated remotely using cloud services and internet facility.

A. Architecture of Cloud based Mobile Forensic Tool

In cloud based mobile forensic tool, the mobile forensic investigator or the cyber forensic expert team can use personal computers or laptops for accessing cloud. In this cloud model the user does not need to purchase hardware, software licenses or implementation services. Mobile forensic investigators can invoke the software and hardware resources in the geographically distributed cloud by dynamic manner. The cloud based mobile forensic tool solves various mobile investigation, analysis and reporting problems encountered daily by the cyber forensic investigator. Therefore, the cloud based mobile forensic tool development is of great importance. Fig. 2 shows the architecture of cloud based mobile forensic tool.

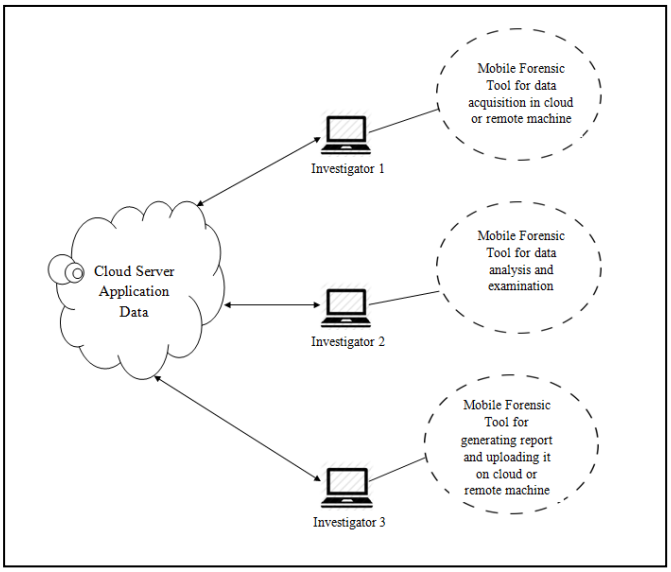

Fig. 2. Architecture of Cloud based Mobile Forensic Tool

In line with cloud computing thinking, around the main function of mobile forensic tool we design the logical structure of cloud based mobile forensic tool as follows.

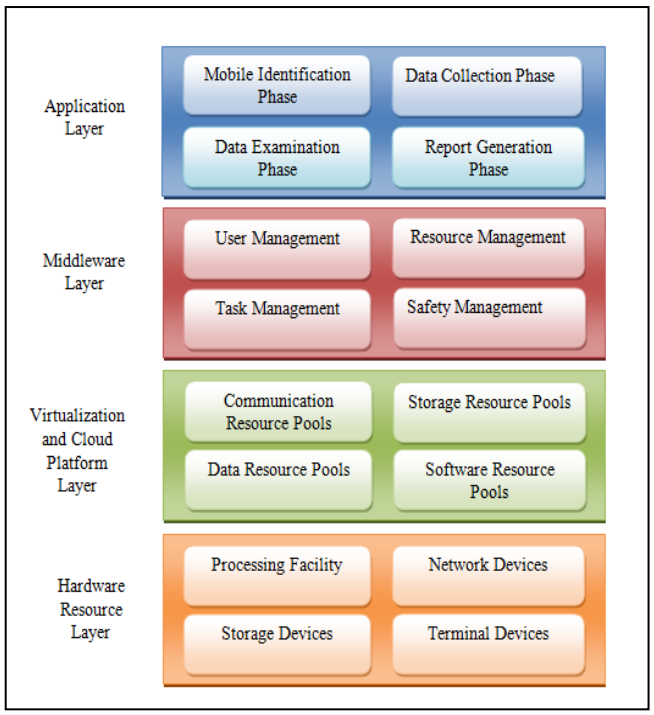

Fig. 3. Logical Structure of Cloud Based Mobile Forensic Tool

This structure divides software system into four logical layers from top to bottom: the application layer, middleware layer, the virtualization and cloud platform layer and the hardware resource layer. [6]

The hardware resource layer includes the hardware resources of the mobile forensic tool. It includes processing facility, network devices, storage devices, terminal devices and so on.

The virtualization and cloud platform layer provides consumers' request for computing resources by using appropriate resources and then deploy huge amount of virtual machine on hardware. The cloud service provider pooled a computing resources to serve large number of consumer's request using dynamically allocation, with different physical or virtual resources is dynamically assigned and reassigned according to the user request. There is a purpose of location independent that the user has no control or knowledge over the actual geographical location of the available resources, but they may be able to identify the location at a higher level of abstraction. [7]

The middleware component layer provides the basic functions of the cloud computing platform, to make sure that cloud services are optimally installed, delivered and maintained. It includes user management, resource management, task management, safety management.

The professional application layer provides needs responsibility in the investigation and analysis of the smartphone contents. SaaS and PaaS is heavily reliant on web application and services. SaaS is typically implemented as a web application and PaaS provides an environment for the development and run time of web application and web services. Associated services and APIs such as managing access for customers are typically implemented using web applications in IaaS [8]. In this model, there are mobile identification phase, data collection phase, data examination phase and report generation phase and so on.

B. Implementation of Cloud Based Mobile Forensic Tool

The Cloud based Mobile Forensic tool is basically split into eight functional modules to address the mobile forensic phases are as follows as given in Fig. 4: Cloud Interface module, Executing Mobile Agent module, Data Acquisition module, Data Analysis module, Data Filtering module, Data Bookmarking module, Hex Viewer module, Report Generation Module. This tool uses Windows Server 2012 as the "Cloud OS", the updated Windows Server is designed for data center scale and the ability to work in concert with Windows Azure to enable support for sophisticated cloud architecture and support for multiple devices.[9]

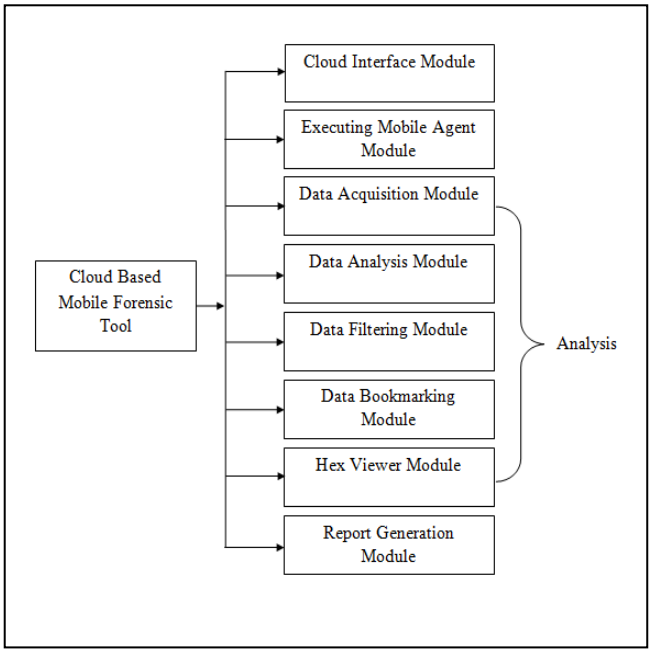

Fig. 4. Implementation of System

C. Advantage of this model

1. *Improves the Security of Cloud based Mobile Forensic Tool:* This model has not only realized the multiple copies of data, but also enhanced the data transmission and improves the security of mobile forensic tool. Even if a particular data is failed or lost, the integrity and authenticity of the mobile forensic data are protected.
2. *Improves Timeliness of Mobile Forensic Tool:* As this tool is geographically distributed, without transmuting into a particular node of the system. When the data send to the cloud, the cloud immediately processes this data in real time. In this way the propagation delay time of client side and server side is reduced. Therefore, it improves the timeliness of the Mobile Forensic Tool.

3. *Easier Resource sharing and Information Integration:* In this model, using virtualization technology, all resources are provided in the upper application software is in a transparent way. Cloud computing stores data on another's computer hardware, removing the need for physical disk on the cloud user site. This model takes advantage of the entire network processing power of cloud computing, significantly speeding up the calculation. So this model can easily share resources and integrate information.

V. CONCLUSION

Even though cloud computing is immature; the standards of security and services are still evolving. The idea of cloud computing will provide a feasible way for the design of mobile forensic tool in the future. Cloud computing would help a cyber forensic expert team achieve efficient use of their hardware and software investments. The purpose of implementing a cloud computing system in mobile forensic is to serve cyber forensics. A cloud based mobile forensic tool is very important in cyber forensic work. But there are many aspects need improvement. We shall continue our work to explore how to make cloud computing to serve mobile forensic better.

REFERENCES

[1] Shivankar Raghav and Ashish Kumar Saxena, "Mobile Forensic: Guidelines and Challenges in Data Preservation and Acquisition", Proceeding of 2009 IEEE Student Conference on Research and Development (SCOReD 2009), 16-18 Nov. 2009, pp 5-8, UPM Serdang.

[2] Khawla Abdulla Alghafli, Andrew Jones and Thomas Anthony Martin, "Forensic Data Acquisition Methods for Mobile Phones", in the 7th Internation Conference for Internet Technology and Secured Transaction (ICITST-2012).

[3] P. Mell & T. Grance. "The NIST Definition of Cloud Computing". NIST Special Publication 800-145. Sept. 2011, pp 2-2.

[4] IBM. "http://www.ibm.com/cloud-computing/us/en/what-is-cloud-computing.html".

[5] Oracle http://www.oracle.com/technetwork/topics/cloud/whatsnew/index-085521.html.

[6] Na Li and Yanhui Du, "Design and Implementation of Cloud Based Forensic Science Information System Model", in 2013 International Conference on Cloud and Service Computing, 4-6 Nov. 2013, pp 140-145, Beijing.

[7] P.Mell & T. Grance. "The NIST Definition of Cloud Computing", NIST Special Publication 800-145. Sept. 2011, pp 2-2.

[8] M.Zhu, "Mobile Cloud Computing: implication to Smartphone Forensic Procedure and Methodologies", Auckland: Auckland University of Technology, 2011.

[9] AMD + Windows Server® 2012 White Paper, "http://sites.amd.com/us/Documents/AMD-WindowsServer_White_Paper.pdf"