A Study of Mobile Cloud Forensics Importance and key Challenges Faced by Investigates

Sameer Dev Sharma, Himani Maheshwari, Shailee Parmar

Abstract*: *Nowadays, Mobile Cloud forensics is the buzzword in the IT market. Everyone is having mobile devices and having his/her crucial data on it. People data is targeted by the hackers to steal the vital information. Mobile devices have limited processing capacity, battery life and storage. But, the cloud computing technology enables the users with indefinite computing resources. Mobile users avail the cloud facilities provided by MCC service provider using SMDs and are charged only on the basis of how much resource they utilize in the cloud (pay-as-you-go). This paper insights an overview of mobile and discuss various challenges faced by the investigators.

Index Terms: Cloud Computing, Cloud forensics, Mobile Cloud Computing, Mobile Cloud Forensics, Smart Mobile Devices.

I. INTRODUCTION

Mobile Cloud Computing (MCC) is a newest architecture that has been developed on the basis of cloud computing to serve the mobile users in a better way. In the present scenario, it is really challenging to live without smart phone. Nowadays almost every individual has a smart phone in which he/she stores his/her potential data. So the users require huge storage capacity and wish to access the data from anywhere and anytime. This led to the development of mobile cloud computing. A number of cloud companies are providing platform for the mobile device users to store their data in cloud and access it with a lot of ease. With the introduction of Mobile Cloud Computing (MCC), the IT infrastructure has changed tremendously from physical to virtual. Smart phone users make use of MCC technology for transferring their personal data to mobile clouds using Smart Mobile Devices (SMDs) [1]. Mobile users avail the cloud facilities provided by MCC service provider using SMDs and are charged only on the basis of how much resource they utilize in the cloud (pay-as-you-go).

Smartphone users feel comfortable with the pay-as-you-go plan to use cloud services. The cloud services can be of three categories such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [2]. Based on their needs, smart phone users choose their preferred service model in terms of utilizing cloud resources. A number of big players in the cloud industry market gain million dollar profit by just renting out their space for Cloud Service Providers (CSP) [3]. Today, most companies invest in millions for cloud services since the organizations shifted their service delivery model into cloud paradigm. Smartphone sellers provide their customers online limited storage though the demand is increasing on a daily basis.

Due to the increasing competition among the CSPs, the users benefit a lot in terms of cloud pricing, advanced features and other benefits etc., According to the literature [4], there is a tremendous increase upto 88% is expected between 2014 and 2018 in cloud computing-based mobile software and applications since there is a huge marginal increase experienced in Mobile Cloud Computing. In parallel to the developments in MCC, the frequency of cyber-attacks too is increasing which directly affects various resources of MCC. There may be various forms of cyber-attacks on MCC, generated by the intruders, such as IoT, DoS, Ad and Click frauds, enterprise-class spyware, application-based attacks, DDoS, network-based attacks, mobile bonnets, physical-based attacks, web-based attacks and Dead apps [5].

There is a tremendous increase experienced in cyber-attacks that target various resources of MCC which results in malicious outcomes. In spite of the fact that some cyber-attacks cannot be tracked, it is possible to trace out such events for redeemable evidence collection [4]. For a forensic expert, it is challenging to trace out the undetected attacks, especially in MCC. In order to get rid of such issues in MCC, digital forensics remains the best optimum solution for investigating the attacks. According to the literature [6], digital forensics is highly helpful in the collection of digital evidence from MCC-based digital devices. It is important to have the digital evidence for the investigator to find out the source from where the attack is initiated. Digital evidence is usually collected by the acquisition of physical devices, though this is not a feasible option in case of MCC since it doesn't use traditional networking. In MCC, cloud remains the only source of information for the digital investigators while at the same time; it is hidden from the investigation. As per the study [7], it is challenging for the forensic investigators to access the resource physically for the purpose of digital data extraction. Moreover, when intruders attack MCC, they either collect or modify the content of the data and also design a number of tools to remove their footprints [8]. In this paper, the researcherprovide insights on MCC and its advantages, digital forensics, difference between digital forensics and mobile cloud forensics, forensics challenges in MCC, future research direction in MCC and conclusion for the discussed topics.

Revised Manuscript Received on May 05, 2019.

Sameer Dev Sharma, Assistant Professor, Department of Computer Science, Uttaranchal University, Dehradun, India.

Himani Maheshwari, Assistant Professor, Department of Computer Science, Uttaranchal University, Dehradun, India.

Sameer Dev Sharma, Lecturer, Department of Management, Uttaranchal University, Dehradun, India.

II. BACKGROUND

A. Mobile Cloud Computing

Mobile devices have limited processing capacity, battery life and storage. But, the cloud computing technology enableS the users with indefinite computing resources. Mobile cloud computing is a hybrid technology created from two components such as cloud computing and mobile devices resulting in the creation of new infrastructure where the cloud performs all the intensive-computing tasks and store huge data. In the hybrid novel architecture, the data storage and data processing occurs outside the mobile devices [9]. MCC refers to the infrastructure where both data storage and data processing occurs outside the mobile device, as defined by MCC forum. In case of mobile cloud applications, the power of data storage and computing are moved out of the devices into the cloud so that the applications are used not only by smartphone users, but also to a wide range of mobile subscribers [20]. MCC enables a platform for the smart phone users who can connect to the mobile web and access their data, applications and other cloud services with ease.

The indigenous characteristics of cloud computing and its advantages are loaded in MCC as well which help the mobile devices get rid of challenges that are usually faced by traditional mobile apps, for instance processing capabilities, data storage etc., According to the literature [2], MCC has a number of advantages in terms of improved ease of integration, data storage, dynamic provisioning, reliability, processing power, scalability and extended battery lifetime. In mobile cloud forensics, two different environments such as terminal and the cloud server should be considered since the applications are executed in cloud server. In parallel, the investigator should look for digital evidence in both mobile and cloud levels.

Advantages of MCC

In a country like India, where one out of three mobiles has less storage capacity or full memory, MCC is highly useful [20].

- Mobile applications can be accessed via cloud thus extending the lifetime of battery and remote processing
- MCC comes with a platform which is convenient for data storage and access of data anywhere at any time. So mobile applications do not trouble the user in terms of storage capacity.
- If a hardware or software failure occurs, the users' data is still safe in the cloud
- MCC provides security mechanism to their users against data theft and virus attacks.
- If the user is continuously moving from one place to another, still they can access their data and services anywhere at any time.
- Data sharing during travel 'on-the-go' and no need to wait for physical access of computing storage devices
- Mobile applications have the enough potential for scaling to meet the growing demands of the users.

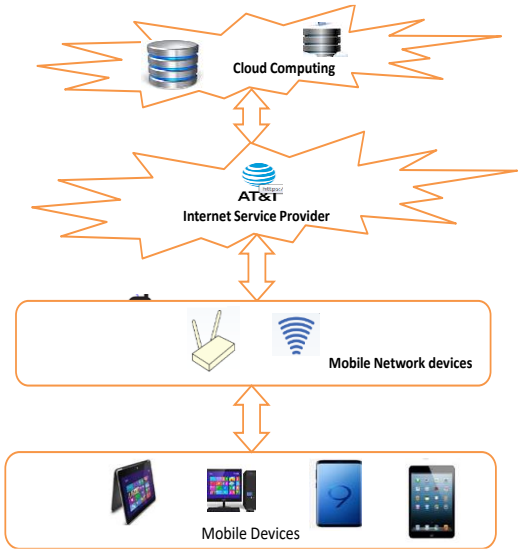

Figure 1: Architecture of Mobile Cloud Forensics

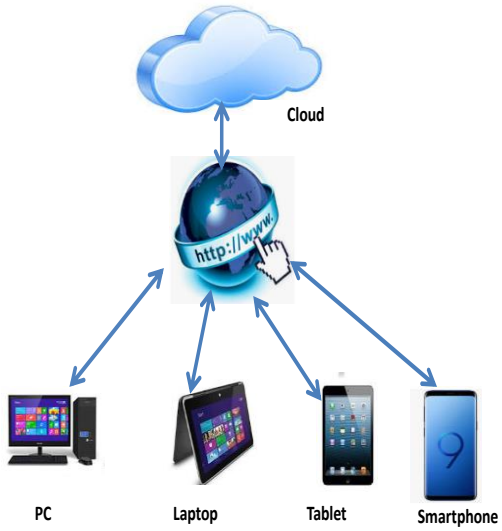

Figure 2: Applications of Mobile Cloud Forensics

What is Digital Forensics?

Digital forensics is a branch of forensic science and is also called as digital forensic science. This branch deals with the recovery and investigation of digital devices and materials related to it as per the governing laws. Digital forensics deals with cyber-crimes in a legal manner and is one of the applications of forensic science. This field has observed a tremendous growth brought by the experienced practitioners who help with cutting-edge research. Researchers are loaded with opportunities from their research work that can be converted into techniques for future purposes. National Academy of Sciences (NAS) published a scathing report calling for a scientific overhaul of digital forensics [15].

Mobile Cloud Forensics

Mobile phone forensics, as the name says, is the forensic science application in mobile phone technology i.e., collection and investigation of digital evidence through legal terms and forensically sound conditions [10].

Mobile data evidence can be of various forms and can be retrieved from external memory card, internal memory, SIM card (Subscriber Identity Module), user mobile device etc. and the collected information would be in the form of short message services, emails, multimedia files, internet browsing history, call history etc. In addition to the above, Network service provider may also provide more information such as call log, user movement and localization over time, and messages information. Brother [12] classified the extraction methods into three such as manual, logical and physical extraction as in a pyramid-like layer. These methods are used by forensics investigators in order to acquire data. Being a pyramid-like structure, it follows bottom-to-top approach i.e., as the extraction procedure narrows down at the top, the process of analysis, technical expertise, time taken for analysis, training, quality of memory images increases.

Cloud forensics is a hybrid technology carved out of two disciplines, digital forensics and cloud computing. Cloud computing can be easily and quickly reconfigured since it is a shared kit of configurable networked resources (e.g., servers, storage, applications, Networks and services) [11]. As per the study [13], digital forensics is a computer science application area where the computer technology is used to recover electronic evidence legally [13].

III. MOBILE CLOUD FORENSICS CHALLENGES

In the current section, the key challenges faced during forensic investigation when handling mobile cloud infrastructure environment are discussed. Mobile cloud forensic experts face a lot of challenges while collecting the data from cloud during a crime. Some of the challenges are discussed herewith.

Lack of forensic tools: For an investigator to collect the digital evidence, appropriate forensic tools are required to collect the information from cloud environment. Such tools so far designed and introduced in digital forensic investigations are not feasible for conducting investigation in SaaS, PaaS, and IaaS models. Though there were few exceptions, there are no proper tools designed for conducting investigation on MCC. So, most of the time investigators deploy the existing tools to investigate the cloud cyber-crimes. It is still under conspiracy that these remove forensic investigation tools are not yet checked for its correctness, error rate or approved legally [14].

Lack of universally accepted standard methods: There are no universally accepted standard methods in the data extraction and internal memory analysis for smartphones. This problem becomes even bigger due to rapid changes in technologies. Every now and then, manufacturers use different methods for storing and processing data in the mobile devices. Rapid upgradation and modifications in Mobile OS: In general, personal computers are installed with Windows OS by the users which are not frequently updated. However, on the other side, mobile devices widely use more operating systems including Apple's most secure iOS, Google's widely used Android, BlackBerry OS, Microsoft Windows Mobile, HP's Web-OS, Nokia's Symbian, and many more. Even within these operating systems, there are number of variants which bring more challenges for the forensic investigator.

Lack of available resources: As discussed earlier, with the growing number of mobile phones, the tools required by the forensic examiner also increases.

Figure 3: Challenges in Mobile Cloud Forensics

Maintenance of device accessories: The devices and its accessories such as device batteries, USB cables and chargers for different mobile phones, have to be maintained in order to acquire information from those devices.

Inhabitation of data modification: No modification in the data is an important and key requirement for the forensic investigation. In other words, during the data extraction from the device under investigation, there should not be any alterations in the data. But with reference to mobile phones, it is not practically possible because one can alter the data by switching the gadget. Even if a gadget is switched-off, the background processes still may run. For instance, the alarm still works in android devices even when it is switched off.

Identification of Data: It is very difficult to track the data in MCC since the 'Virtualize and Distributive notions' create a number of hindrances to digital investigators while tracking data in large distributed cloud environment. In MCC, the accessibility to physical resources is one of the key factors during the data identification process [16]. The service provider's permission is required for accessing the resources that are scattered in the cloud.

Time Mismatch: Time synchronization is another challenge for the investigator since different logs are placed in different countries at different data centers [16]. The evidences collected from cloud need to be proven in courts against the interloper which is one of the most tough tasks because the investigators may receive two different logs for the same task, placed on different locations with different time recordings. It is also challenging to retrieve various logs from various data centers, for instance, the chances are less for the interlopers to alter the logs retrieved from the closest data center, while it may not be the case in the data centers that are far away i.e., chances are high[2].

Complexity of testimony: The investigator process and the steps followed during the investigation need to be explained before the judge in a much simpler manner that makes them understand the entire process since the information is collected by the investigator through many complex steps and the jury mostly has less or scanty knowledge about the computers.

So, it is important for the investigator to make the judges understand the investigation process in a simple manner [17].

Encryption: A number of cloud customers store their data in all the service models discussed above through encrypted format. This is performed so as to protect the data from cyber-crimes. Investigation of an encrypted information is a challenging task since it requires the investigator to possess strong skills in terms of encryption and forensics [18]. During an investigation, the data encrypted remains unused if the investigator cannot acquire the encryption key. In an instance where the data owner lost the encryption key, it becomes even more challenging. A number of CSPs utilize different encryption methods for storing their clients' data in the cloud [19].

Documentation: Documentation of the information collected during investigation and convincing the judge with the collected information are the biggest challenges for the investigator because the judge need to trust that the data recovered had undergone no changes during the history of the trial. During the investigation, the investigators must ensure all the parties are involved and the investigation is conducted as per standard methods, principles so as to ensure the custody of evidence collected [21].

IV. CONCLUSION

This research articles provides an overview of MCC and the advantages associated with it. The article discusses about the prominent forensic challenges faced by MCC so as to prevent intruders. These challenges occur mainly due to virtualization in MCC architecture and distributed characteristics. During the process of investigation, the digital forensics investigators are provided with less authority and scanty MCC resources. But, there needs to be a flexible and legally standardized rule in place to overcome the challenges faced by digital forensic investigators in MCC paradigm. The paper extends in the future with special emphasis on investigation of user identity in MCC environment and definition of identity management scheme in order to find the identification of malevolent users while conducted forensic investigation process.

REFERENCES

1. M. Shiraz, A. Gani, R. H. Khokhar, and R. Buyya, "A review on distributed application processing frameworks in smart mobile devices for mobile cloud computing," Communications Surveys & Tutorials, IEEE, vol. 15, pp. 1294-1313, 2013.
2. Suleman khan1, 2, Ejaz Ahmad1, 2, Muhammad Shiraz1, 2, Abdullah Gani1, 2, Ainuddin Wahid, Mustapha AminuBagiwa2 2014 IEEE 2014 International Conference on Computer, Communication, and Control Technology (I4CT 2014), September 2 -4, 2014 - Langkawi, Kedah, Malaysia.
3. I. Goiri, J. Guitart, and J. Torres, "Characterizing cloud federation for enhancing providers' profit," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010, pp. 123-130.
4. H. Qui, A. Gani, "Research on mobile cloud computing: review, trend and perspective", Second International Conference on Digital Information and Communication Technology and its Applications (DICTAP), 2012.
5. A. Karim, R. B. Salleh, M. Shiraz, S. A. A. Shah I. Awan, and N. B. Anuar, "Botnet detection techniques: review, future trends and issues," 2014.
6. J. Lee, "Pervasive forensic analysis based on mobile cloud computing," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 572-576.
7. K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in Advances in digital forensics VII, ed: Springer, 2011, pp. 35-46.
8. J. Stüttgen and M. Cohen, "Anti-forensic resilient memory acquisition," Digital Investigation, vol. 10, pp. S105-S115, 2013.
9. https://www.ibm.com/blogs/cloud-computing/2013/06/mobile-cloud-computing/
10. NIST Special Publication 800-101, "Guidelines on Cell Phone Forensics", May 2007
11. K. Kent, S. Chevalier, T. Grance and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, Special Publication 800-86, National Institute of Standards and Technology, Gaithersburg, Maryland, 2006.
12. S.Brothers, "Cell phone and GPS Forensic Tool Classification System", Presentation to Digital Forensics, May 2009.
13. P. Mell and T. Grance, The NIST Definition of Cloud Computing (Draft), Special Publication 800-145 (Draft), National Institute of Standards and Technology, Gaithersburg, Maryland, 2011.
14. Dykstra J. Seizing electronic evidence from cloud computing environments. In Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ruan K (ed). Hershey: IGI Global, 2013; 156–185.
15. National Research Council. Strengthening Forensic Science in the United States: A Path Forward. The National Academies Press, February 2009.
16. K. Ruan, J. Carthy, T. Kechadi, and M. Crosbie, "Cloud forensics," in Advances in digital forensics VII, ed: Springer, 2011, pp. 35-46.
17. Dykstra J. Seizing electronic evidence from cloud computing environments. In Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ruan K (ed). Hershey: IGI Global, 2013; 156–185.
18. Adams R. The emergence of cloud storage and the need for a new digital forensic process model. In Cybercrime and Cloud Forensics: Applications for Investigation Processes, Ruan K (ed). Hershey: IGI Global, 2013; 79–104. 29. Kohn MD, EloffMariki.
19. Almulla S, Iraqi Y, Jones A. Cloud forensics: a research perspective. In Innovations in Information Technology (IIT), 2013 9th International Conference on. IEEE, 2013; 66–71.
20. Sibiya G, Venter HS, Fogwill T. Digital forensic framework for a cloud environment. In Proceedings of IST-Africa 2012 Conference. IIMC: Tanzania, 2012.
21. http://www.business-standard.com/article/current-affairs/india-s-love-for-good-morning-msgs-is-slowing-down-your-smartphone-118012300190_1.html
22. Stavros Simou1*, Christos Kalloniatis1, Stefanos Gritzalis2 and Haralambos Mouratidis3A survey on cloud forensics challenges and solutions SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks (2016) Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1688

Author Profile

Sameer Sharma is working with Uttaranchal University Dehradun as an Asst. Professor in the department of Computer Application. He has more than 12 Years of teaching and 3 years of industry experience. He is MCA and M.Phil in Computer Science. He has published a book on e-Governance. His research interest is AI, Expert Systems, Cloud Forensics, Mobile Forensics and Big Data.

Dr. Himani Maheshwari is an Assistant Professor in the Department of Computer Applications, Uttaranchal University, Dehradun. She received her Master of Computer Applications degree with honors from Uttar Pradesh Technical University and PhD degree from Indian Institute of Technology (IIT) Roorkee. Her area of interests is Big Data, Machine Learning, AI and GIS. She has published more than 13 Research Papers in various International Journals & Conferences.

Ms. Shaile Parmar is working with Uttaranchal University Dehradun as Lecturer in the Department of Business studies since 2017. Her area of interest is Marketing Management, Consumer Behavior and Business Communication. She had completed her MBA from Doon University, Dehradun