ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse333942020.pdf
https://doi.org/10.30534/ijatcse/2020/333942020

Mobile Cloud Correlated Digital Forensic Process Model based on UML Design

Puneet Sharma[1], Deepak Arora[2], T.Sakthivel[3]
[1,2] Dept. of Computer Science and Engineering, Amity University, Uttar Pradesh,India
[3]Firstsoft Technologies Private Ltd., Chennai,India
puneetgrandmaster@gmail.com[1], deepakarorarainbox@gmail.com[2], sakthi@firstsoftech.com[3]

ABSTRACT

The world-wide acceptance of inexpensive and powerful smartphones significantly influences the everyday exercise of human lives due to the availability of a vast range of Mobile Cloud (MC) applications. The misuse of cloud-based mobile application services is the most critical evidential hotspot for forensic practitioners. Establishing an MC correlated forensic process model is inevitable to investigate the criminal activities and speed up the forensic investigation process. This paper proposes a correlated process model from the foundation of traditional forensic models to make the MC forensic process more efficient and accurate. This work devises an MC correlated forensic process model with the support of unified modeling language design to capture the dynamic behavior and incorporates the inter-application analysis of cloud-based mobile applications. This process model correlates the forensic-rich evidence in mobile applications and significantly enables the data traceability of the cloud forensic investigation by employing the metadata. The proposed forensic process applies the logical analysis based evidence interpretation, and time synchronization is useful for maintaining a sequential timeline of evidence that correlates the possible evidence concisely. The correlated process model of MC forensic investigation significantly improves the efficiency of the investigation.

Key words: Digital Forensics, Mobile Cloud Forensics, Forensic Process Model, and UML

1. INTRODUCTION

Modern life relies on Information and Communication Technologies (ICT) and digital devices that enable a rapid explosion of digital crimes around the world. This significantly increases the demand for digital forensic investigation from law enforcement agencies to prove the crime. The rapid expansion of modern technologies and their cloud-based distribution of various devices is a significant hurdle in the investigation process. Cybercriminals employ highly sophisticated attacking mechanisms by utilizing advanced technology and distributed devices across different digital networks and regions. Thus, it is essential to develop standard forensic tools and methods to support the rapidly evolving digital technology [1] [2]. The shortage of forensic tools and experts for emerging technologies significantly increases the backlog of investigation in recent times [3]. The rapid evolution of smartphones and cloud computing has significantly changed the landscape of application models [4]. Cloud-based mobile applications play a significant role, enabling users to interact with other organizations, communities, services, and individuals globally. A complete survey focuses on forensic analysis of MC applications and collects potential evidence from the perspective of forensic investigations [5]. In essence, effectively analyzing the artifacts of cloud based on mobile evidence for online and offline activities is a significantly challenging task due to a large number of unlawful activities in the MC applications [6]. In addition, the lack of standardized forensic processes and the massive volume of data to be analyzed during forensic investigation degrades the performance of the investigations, notably in the MC environment [7].

The digital forensic process model has to undergo significant changes to cope up with the rapid advancement of technology. The digital forensic practitioners have developed different investigation models in the fields of computer forensics, network forensics, device forensics, and cloud forensics. Several research groups such as the Technical Working Group on Digital Evidence (TWGDE), the Scientific Working Group on Digital Evidence (SWGDE), the National Institute of Justice (NIJ), and the Computer Analysis and Response Team (CART) have discussed the computer forensic science and suggest for the standardization of forensic process model [8]. In the digital investigation, each country and organization develop its forensic investigation procedures to focus on data analysis and technology aspects of the investigation [9].

Digital forensics [10] employs the different scientifically proven and derived methods towards the identification, preservation, acquisition, analysis, interpretation, presentation, and validation. UML is a preferable paradigm by forensic researchers or investigators to model the digital forensic processes from the perspective of the structural and behavioral model. UML modeling has been used by the proposed model to describe the forensic processes involved

in the mobile, cloud, and MC environment. The primary objective is to design a new forensic process which is the result of the normalization of the existing mobile and cloud forensic process models. The proposed forensic model correlates the essential components in the digital forensics process to support the investigation of the malicious activities in the MC applications. It models the fundamental forensic components and their functional relationships by applying the UML. The UML diagrams effectively visualize the forensic activities, and the proposed MC correlated model utilizes the capabilities of UML. The proposed correlated forensic process significantly improves the forensic procedure of MC applications and models the enriched forensic process model using the UML diagrams. This work unifies and exemplifies the enriched forensic procedures for the MC correlated model with the assistance of the UML diagrams.

The rest of the paper is organized as follows. Section 2 discusses the related works of mobile forensics, cloud forensics, and MC forensic process models. Section 3 describes the preliminaries, including the definitions of the forensic components and UML models. The proposed MC correlated forensic process model is briefly exemplified in the Section 4. The UML modeling for the proposed forensic process model is presented in Section 5. Section 6 concludes this work.

2. BACKGROUND STUDY

This section reviews several existing forensic process models in digital forensics, cloud forensics, and mobile forensics. Furthermore, it discusses the forensic processes employed in the investigation of MC applications.

The numerous available forensic procedures model the investigation against unauthorized actions or unlawful criminal activities. Moreover, the research committees such as the American Society of Digital Forensics and eDiscovery (ASDFED) [11] and Digital Forensic Research Workshop (DFRWS) [12] have presented different forensic procedures to support the collection of digital evidence. Investigating the crime event with the standard forensic procedure is significant. A formal modeling approach is essential to represent the digital forensic process model in terms of the investigative process and phases involved. A flow thing based specification methodology proposed an abstract model for a digital forensic process to avoid informal approaches [13]. It uniformly specifies the flow thing-based model for various processes and established phases of the digital forensic investigation. Paper [14] introduced a formal modeling approach for the forensic process model by applying the Unified Modeling Language (UML) modeling approaches [15].

The digital forensic researchers have introduced different forensic procedures for conducting computer forensics, network forensics, and mobile forensics with the consideration of the legal standards. Malaysian Investigation Process-based digital forensics model [16] has focused on the data acquisition process involving the static data and live data acquisition and presented the forensic processes based on the Malaysia Cyber Law. Systematic Digital Forensic Investigation Model (SRDFIM) [17] proposed a complete model that inspires DRFWS Digital Investigation Model to offer a consistent and systematic approach for forensic investigations. By modeling the eleven-stage forensic processes, it assists the organizations and forensic practitioners in performing the appropriate forensic procedures systematically.

The integrated Digital Forensic Process Model in paper [18] applied five major forensic stages in digital forensic investigation such as forensic preparation, incident and incident response, and finally the presentation. It discusses the possibility of adapting the investigation procedures of the physical crime to the forensic processes of the digital crime scene. A practical Mobile Forensic Investigation (MFI) life cycle model [19] addresses the significant challenges faced by the existing forensics procedures by employing new methodologies to enable the useful process model for forensic life cycle. The mobile forensics method in [20] utilizes the effective digital investigation process to extract the potential evidence from the mobile device. A multi-stage investigation model with various processes called Smartphone Forensic Investigation Process Model (SPFIPM) presented in [21]. A cloud forensic process model called Forensic Process as a Service (FPaaS) in [22] employs the cloud-based Business Process Execution Language (BPEL). An integrated digital forensic framework is presented in [23] that tackles the significant challenges in the investigation of cloud forensics. According to the forensic standards, it initially collects the login credentials or caches from the physical device and acquires the related evidence from the cloud environment.

To design a new forensic process model on MC forensics, identifying the forensic elements in all possible aspects is essential. From the analysis of the existing mobile and cloud forensics literature, this section presents the most critical forensic components and the key concepts of the UML representation. This paper is the extension of our previous work [24].

In the MC infrastructure, the crime event or incident involves the possession of cyber espionage, ransomware, child pornography, fraud, leakage of sensitive information, terrorist activities, or Distributed Denial of Service (DDoS) attacks. An MC user commits any crime on their smartphone while accessing the cloud-based mobile application. The MC correlated forensic process model of this paper involves several entities such as Crime Event, forensic process, Forensic Investigator or Forensic Examiner, Evidence, Chain of custody, Suspect, External Malicious Individual, Cloud Service Provider, Forensic Report, and Law Enforcement Officer. This work assumes that cloud service providers, forensic investigators, and law enforcement officers are trusted, whereas the cloud user and external malicious individuals are not trusted. The forensic investigators or forensic examiners belong to either incident response teams, law enforcement agents, or other individuals or groups in legal or human resource departments.

The UML [15] is a formal language for conceptual modeling of a wide range of systems that include digital forensics to visualize and construct the artifacts. It is more expressive to address the different perspectives of the artifacts applied to the digital forensic process model. The primary building blocks and mechanisms employed by the UML is more appropriate to express the components and phases of the digital forensic process [14]. The vocabulary and rules of the UML help the forensic investigator to understand the representation of the forensic model systematically. It can adequately express and capture the structural and behavioral aspects of the forensic systems. UML provides a set of diagrams to visualize the graphical representation of elements. The UML diagrams are more significantly capturing the artifacts of digital forensic models such as use case diagram, interaction diagram, statechart diagram, activity diagram, component diagram, and deployment diagram.

3. SYSTEM MODEL

Figure 1 depicts the outline of the software prototype of the MC correlated forensic process model. The system model consists of an OpenNebula cloud environment deployed with an Android application. Initially, to implement the process, two different desktop machines installed with Ubuntu 16.04 LTS for the installation of the OpenNebula cloud and Android client. In the android system, the files, applications, and activities are modeled as similar to the android smartphone. In the OpenNebula system, the entire cloud set up is modeled with the application server, database server, web server, storage, files, folders, and virtual machines. Let the Android client access the OpenNebula cloud to perform computation-intensive or resource-intensive tasks on the cloud. The cloud-based mobile application is executed on the Android client, and the corresponding logs are stored in both the mobile storage and cloud storage.

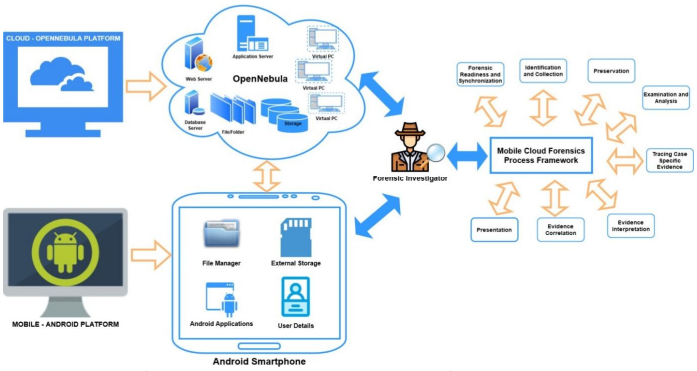

Figure1: Software Prototype Architecture of the MC Correlated Forensic Process Model

For the implementation of the forensic model, the Android client involves the launching of malicious activity during the execution of the cloud-based mobile application. According to the procedure involved in the MC forensic process framework, the model sequentially performs the forensic investigation steps in the correlated MC environment. The MC forensic process framework enforces the investigator to acquire and investigate the mobile artifacts from the android platform and the cloud artifacts from the OpenNebula platform based on the enhanced phases in the forensic framework, which tends to the intelligent forensic decision-making.

4. THE MC CORRELATED FORENSIC PROCESS MODEL

This section exemplifies an enhanced MC forensic process model and its sequential processes with the help of process flow diagrams. The correlated MC forensics notably decomposed into several pre and post-investigative process capabilities to support the complete life cycle. The proposed methodology predominantly focuses on multiple phases. It includes many phases in the traditional forensic process after completing the forensic readiness with the synchronization phase [25]. The standard time synchronization phase supports the exact tracing of the specific mobile and cloud data by examining the inter and intra-application [26]. Finally, it incorporates evidence interpretation and evidence correlation processes for improving decision making in the MC forensics. Figure 2 shows the overall forensic procedures of the proposed MC forensic process model.

4.1. Forensic Readiness

To minimize the risks during the investigation and enhance the quality of evidence, the preparation or forensic readiness phase is planned out, as discussed in [25]. In MC forensics, forensic readiness is the pre-investigation process. As appeared in Figure 3, the readiness contains sub-phases such as management of identity, event, encryption, and interoperability.

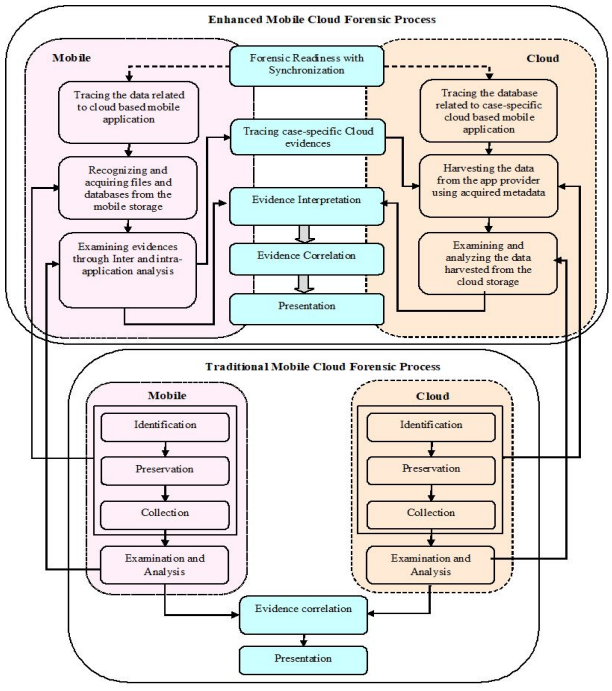

Figure 2: The Mobile-Cloud Correlated Forensic Process Model

The proposed model applies a digital forensic readiness component to the Smartphone and Cloud instance as a part of the solution to enhance the traditional process by time synchronization.

Figure 3: An Outline of the Forensic Readiness Process

It improves both the exactness and time productivity by viably taking care of the mobile and cloud forensic artifacts before starting the forensic examination. The steps involved in the forensic readiness phase is depicted in Figure 4.

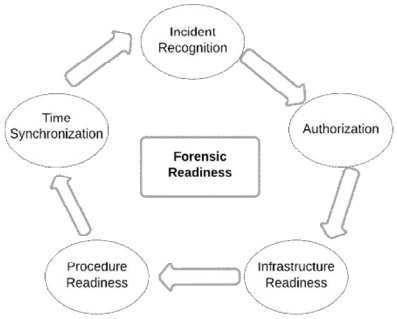

Figure 4: Forensic Readiness Phase

4.2. Identification and Collection

The acquired MC forensic artifacts are the input for mobile and cloud forensic examination and analysis processes, respectively. In a mobile device, evidential artifacts refer that the user activities on the application and SIM in the form of backup files, and chat logs. The evidence in the cloud is in the form of virtual machine images, files, and logs that are retrieved from the cloud service providers. This phase is also associated with the preservation phase for protecting the integrity of the evidence until the evidence submitted to the court. Thus, it helps to maintain the integrity and ensure the originality of the evidence throughout the investigation in the MC.

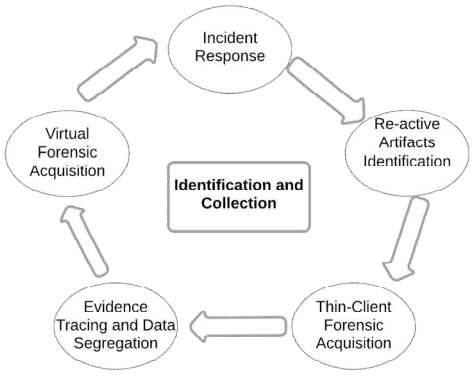

Figure 5: Identification and Collection Phase

The proposed forensic model considers several essential processes in the identification and collection phase, which are shown in Figure 5. The incident response involves data preservation related to criminal events in either mobile or cloud. Reactive artifacts identification and collection is the process of triggering the forensic artifact collection after a crime incident. The proposed model acquires mobile artifacts by searching and locating electronically stored information.

4.3. Examination and Analysis

In the MC scenario, examination and analysis phase employs the acquired forensic artifacts from the mobile and cloud. The assessment of forensic artifacts principally performs data extraction from the crime event and reduction of data to encourage the next phase of forensic analysis. Identifying and correlating the relationship between the mobile and cloud artifacts is the primary process of analysis. Analysis is responsible for the timeframe analysis, file analysis, hidden data analysis, and application analysis. The data reduction process significantly minimizes the amount of data to be analyzed that associated with examination and analysis.
The proposed forensic process assembles the improved mobile analysis phase to facilitate the proof acquisition in the cloud, which is illustrated in Figure 6.

4.4. Evidence Interpretation, Correlation, and Presentation

The last phase of the investigation procedure in the MC environment is evidence interpretation, correlation, and presentation. The focal point of the MC investigation choice depends on the proof understanding and connection between the evidential artifacts of mobile and cloud. The chain of custody data demonstrates the soundness of evidence which is maintained by the forensic investigator.

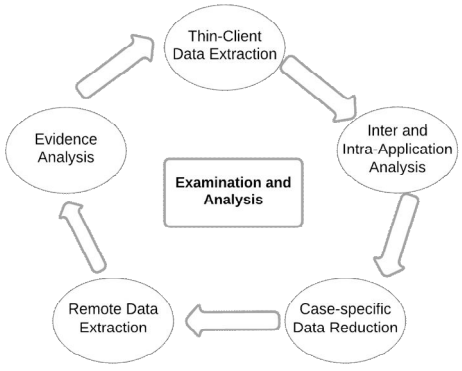

Figure 6: Examination and Analysis Phase

Figure 7 illustrates the components involved in the interpretation, correlation, and presentation processes. In the evidence interpretation, the proposed forensic process model logically analyzes the fine-tuned mobile evidence correlates to cloud evidence that facilitates decision making in the court.

The correlated forensic model maintains the chronological timeline of events for both the mobile and cloud proof to encourage the proof relationship sequentially. To check the proof that is identified with the comparing crime and the suspect, the MC forensic model corresponds to the examined potential artifacts related to the file type and timestamp.

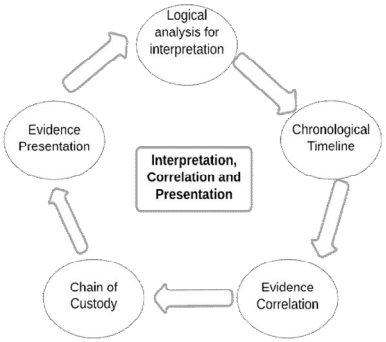

Figure 7: Correlation and Presentation Phase

5. APPLYING UNIFIED MODELING LANGUAGE (UML) TO THE PROPOSED MC CORRELATED FORENSIC PROCESS MODEL

The representation of the proposed MC forensic process model encompasses the formal representation of UML, a set of forensic principles, and the operating procedures. UML diagrams define the process flows of the forensic investigation in the MC forensic model. Owing to the existence of the informal representation in digital forensics, several works [14, 27] have suggested the formal modeling approach of the UML for the digital forensics process models. The research work [28, 29] concludes that the UML is crucial to define the high-level processes in the digital forensics investigation due to the de-facto standard modeling language of the UML. Accordingly, to describe the forensic process in the proposed process model, this work develops the utilization of UML in the MC forensics with the help of the UML diagrams such as a component diagram, deployment diagram, activity diagram, and sequence diagram.

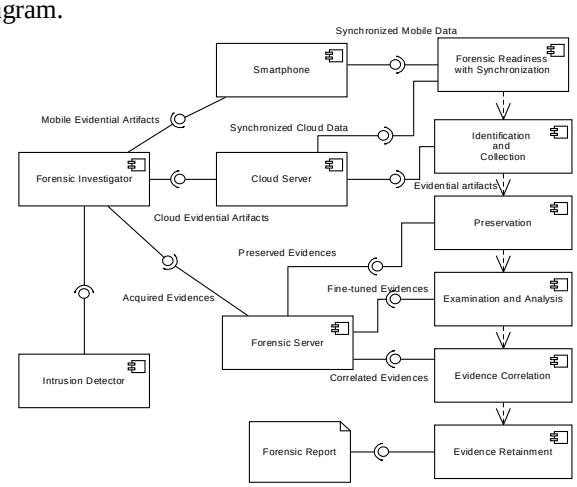

Figure 8: Component Diagram of the MC Correlated Forensic Process Model

To model the static aspects of the software system, the proposed process model employs the component diagram that describes the forensic components involved in the MC forensic investigation process. The detailed view of the forensic investigation process from the phase of time synchronization to the evidence correlation and presentation phase in the MC environment is shown in Figure 8 with the consideration of the components and interfaces of the component diagram.

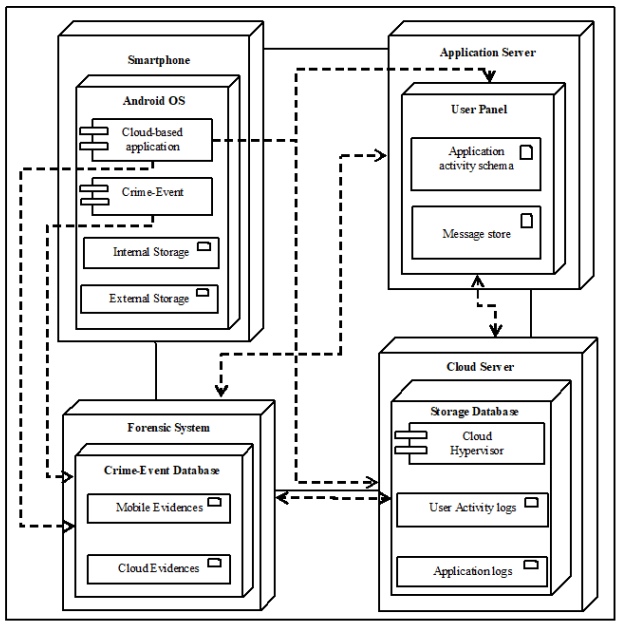

Figure 9: Deployment Diagram of the MC Correlated Forensic Process Model

Figure 9 depicts the deployment diagram of the MC - Correlated digital forensic process model. With the help of the forensic server, the forensic investigator is responsible for conducting the entire forensic investigation in the MC environment. Smartphone and cloud server comprises the potential evidence regarding the crime event, which are acquired by the investigator with the help of the cloud service provider and application service provider that is potential information is extracted from the cloud server and application server, respectively. In essence, the forensic investigator extracts the artifacts related to the cloud-based mobile application of the suspect, which are stored as the application activity schema and message store for a specific user in the application server. From the cloud server, the user activity logs and application logs are extracted about the crime event launched mobile application along with the applications installed by the suspect.

Figures 10 illustrates the UML activity diagram of the proposed MC forensic process model. The activity diagram is one of the five dynamic modeling diagrams in the UML, which is in the form of a flowchart revealing the control flow from one activity to another activity in the software system. In the UML activity diagram, the term activity represents an ongoing dynamic execution within the

software system, which is the incorporation of the executable static computations. The activity diagram is not only used for modeling the dynamic aspects of the software system but also used for building the executable systems based on the forward and reverse engineering. The construction of an activity diagram depends on several shapes connected with arrows. In the activity diagram, the black circle represents the start of the computational process in the software system, ellipses refer to the actions, diamonds indicate the decisions, bars denote the start or end of the sequential activities, and the enriched black circle refers the end of the computational process. With the target of modeling the entire forensic investigation process in the proposed model, this work exploits the activity diagram for the representation of the forensics model in the MC environment.

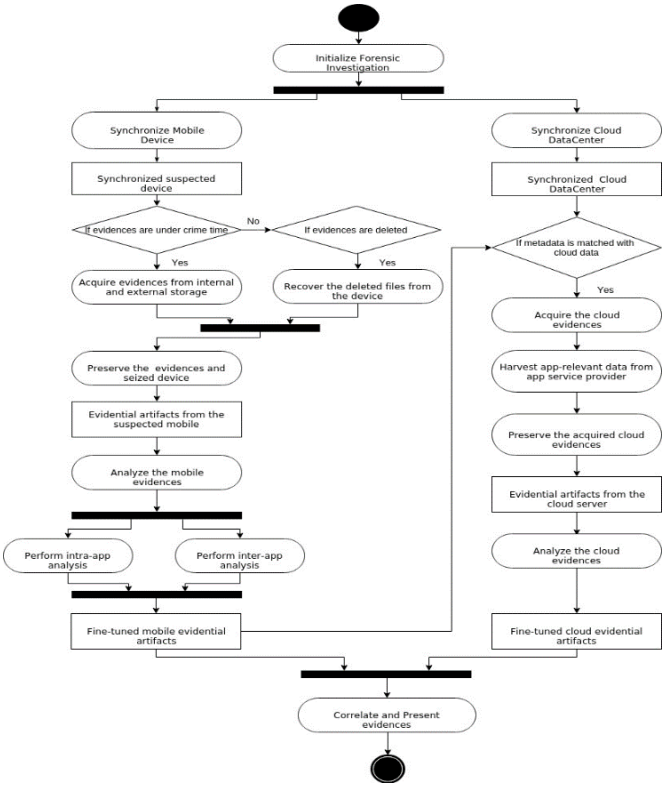

Figure 10: Activity Diagram of the MC Forensic Process Model

In the UML diagram, a sequence diagram is also referred to the interaction diagrams, modeling the dynamic process of the software system. Interaction diagrams illustrate the interactions among a set of objects using the messages for process understanding and arrows in the flow direction. The sequence diagram highlights the software processes in the time ordering manner. It plays a crucial role in modeling the concrete instances of the interfaces, classes, nodes, and components with the help of the messages for denoting the dispatch process among the objects, which illustrates the behavioral pattern of the software system. Similar to activity diagrams, sequence diagrams are also used for both modeling the dynamic aspects of the system and building the executable systems.

A sequence diagram is the projection of the objects and their roles through sequencing links and messages. Figure 11 depicts one of the interaction diagrams in UML, such as a sequence diagram for describing the proposed MC forensic process model. By utilizing the forensic investigator, mobile device, cloud service provider, application service provider, cloud server, forensic server, and law enforcement officer as the objects in the sequence diagram, this work model the sequential activities among these objects with the forensic processes in terms of dispatch messages in the MC environment. Finally, the law enforcement officer is responsible for validating the conducted investigation using the submitted evidence and the chain-of-custody information, which is presented by the investigator.

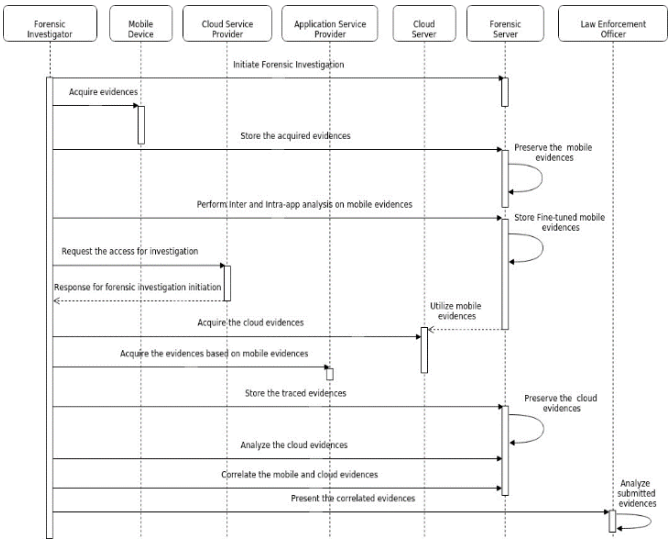

Figure 11: Sequence Diagram of the MC Correlated Forensic Process Model

5.1. UML Diagrams of the Forensic Sub-Phases in MC Correlated Forensic Process Model

This section applies the statechart diagram for two sub-phases, such as the examination and analysis in the mobile device and the evidence correlation in the MC environment.

5.1.1. Forensic Examination and Analysis Process in Mobile

The MC correlated digital forensic process model enriches the forensic examination and analysis process in the mobile device with the intra and inter-app analysis process. Figure 12 illustrates the statechart diagram for the forensic examination and analysis phase in the mobile device. This phase generates the fine-tuned mobile evidence from the

acquired evidential artifacts of the internal and external storage of the suspect's smartphone. To accomplish this objective, the proposed forensic process model performs intra and inter-application analysis. With the target of extracting the crime event that is case-specific data and behaviors of the suspect, it performs the intra-application analysis, which is executed within the crime-event launched application. In subsequent, it focuses on the inter-application analysis between the crime-event launched application and other cloud-based mobile applications installed by the suspect in the seized mobile device. Consequently, the proposed forensic process model obtains the implicit behavioral information about the suspect and their trust value. Finally, it retains the case-specific and potential evidence alone by filtering the raw evidence based on the intra and inter-application analysis.

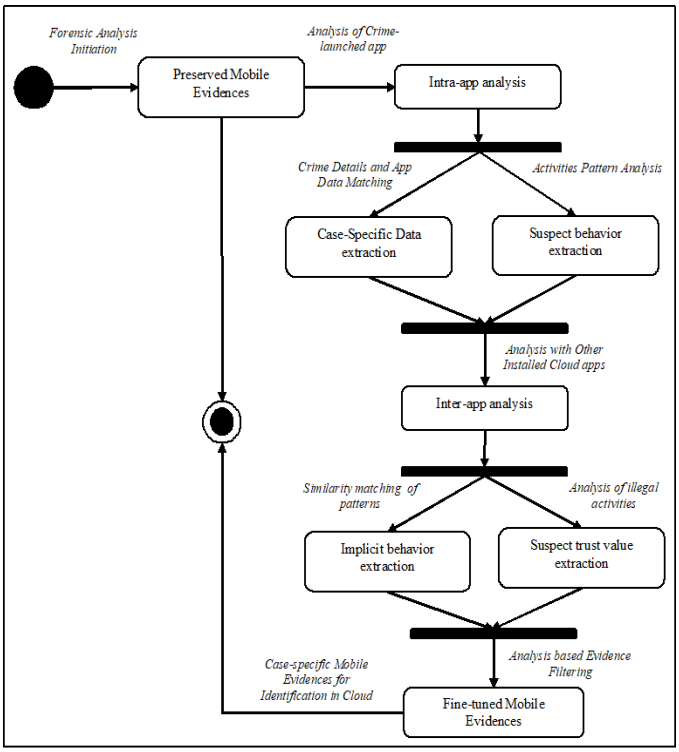

Figure 12: Statechart Diagram of the Proposed MC Correlated Forensic Examination and Analysis

5.1.2. Forensic Evidence Interpretation and Correlation Process in MC Environment

With the target of improving forensic decision-making, the proposed forensic process model incorporates the evidence interpretation and evidence correlation processes for the fine-tuned MC evidence. The detailed events and states of the evidence interpretation and evidence correlation processes are illustrated in Figure 13.

To realize the potential value of the forensic evidence, the proposed forensic process model applies the evidence interpretation process on both the mobile and cloud evidence. The evidence interpretation allows valuable forensic evidence to assist the court during decision making regarding a crime event. In the context of the court, the proposed forensic process model improves the understanding value of the mobile and cloud evidence, which facilitates the reconstruction of the crime event, and decision making. After recognizing the strength of the evidences, it correlates the mobile and cloud evidence based on the chronological ordering of the timeline. Thus, the proposed forensic process model outcomes the valuable and correlated MC evidence for further decision making.

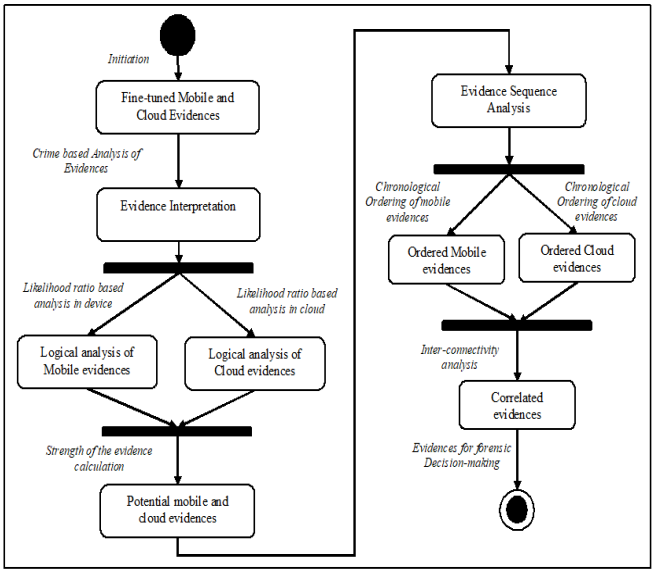

Figure 13: Statechart Diagram of the MC Forensic Evidence Interpretation and Evidence Correlation Process

6. CONCLUSION

The MC correlated forensic process model is presented in this paper for improving the performance of cloud-based mobile application forensics. It unifies the forensic process models of mobile and cloud by applying UML modeling language to support MC forensic investigations. UML diagrams capture the process flows of the forensic process to show the multiple views of the process. The efficient time synchronization along with inter and intra-application analysis significantly improve MC forensic procedures. Time synchronization-empowered forensic analysis of the mobile device improves proof acquisition in the cloud. Moreover, the proposed forensic process model assists the crime event reconstruction and decision making in the court by incorporating the evidence interpretation and evidence correlation processes. Thus, it improves the overall investigation performance during application forensics in the MC environment.

REFERENCES

[1] Simson L. Garfinkel. **Digital forensics research: The next 10 years**, *Digital Investigation*, Vol 7, Supplement, pp s64-s73, 2010.

[2] Damshenas, M., Dehghantanha, A., Mahmoud, R. **A Survey on Digital Forensics Trends**, *International Journal of Cyber-Security Digital Forensics*, Vol,3, pp.1–26, 2014. https://doi.org/10.17781/P001347

[3] Lillis D., Becker, B., O'Sullivan, T. and Scanlon, M. **Current challenges and future research areas for digital forensic investigation**", *arXiv preprint arXiv:1604.03850*, 2016.

[4] Atta ur Rehman Khan, Mazliza Othman, Sajjad Ahmad Madani, and Samee Ullah Khan. **A Survey of Mobile Cloud Computing Application Models**, *IEEE Communications Survey & Tutorials*, VOL. 16, NO. 1, pp 393-413, 2014.

[5] Faheem M., Kechadi, T. and Le-Khac, N.A. **The state of the art forensic techniques in mobile cloud environment: A survey, challenges and current trends**, *International Journal of Digital Crime and Forensics (IJDCF)*, Vol.7, No.2, pp.1-19, 2015.

[6] Khan S., Ahmad, E., Shiraz, M., Gani, A., Wahab, A.W.A. and Bagiwa, M.A. **Forensic challenges in mobile cloud computing**, *IEEE International Conference on Computer, Communications, and Control Technology (I4CT)*, pp.343-347, 2014.

[7] Du, X., Le-Khac, N.A. and Scanlon, M. **Evaluation of digital forensic process models with respect to digital forensics as a service**, *arXiv preprint arXiv:1708.01730*, 2017.

[8] United States, Office of Justice Programs, **Forensic examination of digital evidence: a guide for law enforcement**, *US Department of Justice, Office of Justice Programs*, National Institute of Justice, 2004.

[9] Liles, S., Rogers, M. and Hoebich, M. **A survey of the legal issues facing digital forensic experts**, In *IFIP International Conference on Digital Forensics*, Springer, pp.267-276, 2009. https://doi.org/10.1007/978-3-642-04155-6_20

[10] Anders O.Flaglien. **The Digital Forensics Process**, *Digital Forensics*, chapter 2, 2017, https://doi.org/10.1002/9781119262442.ch2.

[11] **The American Society of Digital Forensics and eDiscovery**, Available Online at:https://asdfed.com/, Accessed on December, 2019.

[12] **Digital Forensics Research Workshop**, Available Online at:https://dfrws.org/, Accessed on December, 2019

[13] Al-Fedaghi S. and Al-Babtain, B. **Modeling the forensics process**, *International Journal of Security and Its Applications*, Vol.6, No.4, pp.97-108, 2012.

[14] Köhn, M., Eloff, J.H. and Olivier, M.S. **UML Modelling of Digital Forensic Process Models (DFPMs)**, In *ISSA*, pp.1-13, 2008.

[15] G. Booch, J. Rumbaugh, and I. Jacobson. **The Unified Modeling Language User Guide**, *Addison Wesley*, 1999.

[16] Perumal S. **Digital forensic model based on Malaysian investigation process**, *International Journal of Computer Science and Network Security*, Vol.9, No.8, pp.38-44, 2009.

[17] Agarwal, A., Gupta, M., Gupta, S. and Gupta, S.C. **Systematic digital forensic investigation model**, *International Journal of Computer Science and Security (IJCSS)*, Vol.5, No.1, pp.118-131, 2011.

[18] Kohn M.D., Eloff, M.M. and Eloff, J.H. **Integrated digital forensic process model**, *Computers & Security*, Vol.38, pp.103-115, 2013. https://doi.org/10.1016/j.cose.2013.05.001

[19] Rajendran, S., and N. P. Gopalan. **Mobile Forensic Investigation (MFI) life cycle process for digital data discovery (DDD)**, *Springer Proceedings of the International Conference on Soft Computing Systems*, pp.393-403, 2016.

[20] Mumba, E.R. and Venter, H.S. **Mobile forensics using the harmonised digital forensic investigation process**, *IEEE Information Security for South Africa*, pp.1-10, 2014.

[21] Goel, A., Tyagi, A. and Agarwal, A. **Smartphone forensic investigation process model**, *International Journal of Computer Science & Security (IJCSS)*, Vol.6, No.5 pp.322-341, 2012.

[22] Eleyan, A. and Eleyan, D. **Forensic Process as a Service (FPaaS) for Cloud Computing**, *IEEE Intelligence and Security Informatics Conference (EISIC)*, pp.157-160, 2015.

[23] Martini, B. and Choo, K.K.R. **An integrated conceptual digital forensic framework for cloud computing**, *Digital Investigation*, Vol.9, No.2, pp.71-80, 2012.

[24] Puneet Sharma, Deepak Arora, T. Sakthivel. **UML-based process model for mobile cloud forensic application framework – a preliminary study**, *International Journal of Electronic Security and Digital Forensics*, Vol. 12, No. 3, pp. 262-278, 2020.

[25] Puneet Sharma, Deepak Arora, T. Sakthivel. **Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications**, *International Journal of Digital Crime and Forensics*, VOL. 12, NO. 3, pp. 58-76,2020.

[26] Puneet Sharma, Deepak Arora, T. Sakthivel. **Enhanced Forensic Process for Improving Mobile Cloud Traceability in Cloud-Based Mobile Applications**, *Procedia Computer Science*, VOL. 167, pp. 907-917,2020.

[27] Bogen, A.C. and Dampier, D.A. **Unifying computer forensics modeling approaches: a software engineering perspective**, *IEEE First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05)*, pp.27-39, 2005.

[28] Ruan, C. and Huebner, E. **Formalizing computer forensics process with UML**, *In International United Information Systems Conference*, Springer, pp.184-189, 2009.

[29] Saxena, V., Arora, D. and Ahmad, S. **Object Oriented Distributed Architecture System through UML**, *In Proc. of Advances in Computer Vision and Information Technology, IEEE International Conference*, pp. 305-310, Aurangabad (MS)-India, 2007.