Comparison of Computer Forensics Investigation Models for Cloud Environment

A. Huseinović* and S. Mrdović**
University of Sarajevo/Faculty of Electrical Engineering, Sarajevo, Bosnia and Herzegovina
ahuseinovic@etf.unsa.ba**, sasa.mrdovic@etf.unsa.ba**

Abstract - ***Computer forensics investigation process evolved from analysis of offline data copies to the process of finding whole spectrum of non-volatile traces in local and remote user environments. Many computer forensic investigations models proposed by researchers and incident respondents were widely accepted for static and live analysis of the systems. With cloud environment surrounding almost every aspect of information technology, researchers find it difficult to apply those models to investigation involved. In this paper, state-of-the-art forensic investigation models for cloud environment have been presented.***

Keywords **– digital** ***forensics; cloud computing; digital investigation; digital evidence;***

I. INTRODUCTION

In last 20 years digital forensic investigators and scientists have developed and proposed many forensic investigation models that were mostly applied to specific investigation sets. In 2001, Palmer at al. defined model that aimed to determine common phases of digital forensic investigation along with definition of key concepts and order of phases. The proposed investigative process is linear and consists of seven phases: *Identification, Preservation, Collection, Examination, Analysis, Presentation* and *Decision* [1]. Palmer at al. addressed open key questions regarding digital forensic science and its future development.

Many researches and forensic investigators proposed process models that extend existing and introduce new phases. New process models tend to be better suited for investigations that authors performed. This results in many different investigation models. Widely accepted models are mentioned in this paper.

On the other side, continuous development of IT related Internet services have evolved to whole new spectrum of services established in cloud environment. This makes it hard for forensic investigators to perform earlier established procedures, in environment that relies on remote resources. These resources may often be available in limited time for analysis due to possible subscription expiration of services, account suspension etc.

The rest of this paper is organized in following mater. Chapter II gives short description of traditional forensic investigation models and their phases. Main restrictions of those models applied to digital forensic investigation determined by researchers is also noted. In Chapter III state-of-the-art models and challenges in cloud environment are discussed. Chapter IV consists of conclusions and future research path considerations.

II. MATURATION OF FORENSIC INVESTIGATION PROCESS MODELS

Recent publications [2], [3], [4], [5] and [6] give brief overview regarding maturation of digital forensics investigation models. All comparisons of models start by giving detailed explanation of models proposed by M. Reith, C. Carr and G. Gunsch [7] along with model proposed by B. Carier and E. Spafford in 2003 [8].

In [2] authors give the short review of models developed prior to models proposed in [7] and [8]. First model described is *Computer Forensic Investigation Process* established in 1984 by FBI, and described by FBI agent M. Pollitt in [9]. This model consists of four phases: *Acquisition, Identification, Evaluation and Admission.* The second model described is one proposed by Palmer et al. [1].

The Abstract Digital Forensic Model proposed by M. Reith, C. Carr and G. Gunsch [7] consists of nine phases: *Identification phase, Preparation phase, Approach strategy selection phase, Preservation phase, Collection phase, Examination phase, Analysis phase, Presentation* phase and *Returning evidence phase*. Main disadvantages of this model are [3]:

- high-level approach to categorisation,
- there is no obvious method to test the model and
- more granularity of categories increases complexity.

The *Integrated Digital Investigative Process*, proposed and developed by Carrier and Spafford [8], involves *Digital Crime Scene Investigation* into *Physical Crime Investigation Phase*. The model consists of seventeen phases divided into five groups: *Readiness Phases, Deployment Phases, Physical Crime Scene Investigation Phases, Digital Crime Scene Investigation Phases* and *Review Phase* [4] [8]. Following this model, investigators should consider digital crime scene as "the virtual environment created by hardware and software where digital evidence of crime or incident exists" [3]. According to [3] the model has been applied to some case studies, but no evidence exists that it has been referenced while creating standards for forensic investigation models. This model is improved by *Enhanced Digital Investigation Process Model* [10] that instead of linear application of phases, represents phases as iterative.

According to authors, its iterative nature helps to trace the computer that has been used as tool to commit offense [10]. In order to prevent ambiguities, this model supports reconstruction only after all of the investigations have been completed.

Extended Model of Cybercrime Investigation, proposed by S. Ciarduhain, [11] is comprehensive model. The information flow between investigation phases is addressed in this model. The investigation activities are conducted in sequences. Iteration of some investigation parts is possible [5].

A Hierarchical, Objectives-Based Framework for the Digital Investigations Process [12] proposed by Beebe and Clark focuses on low-level activities of digital investigation. This is opposite to abstract concepts defined in previous models. Two contributions of this model [3] are „multi-tier" approach and introduction of *Principles* defined as high level procedures applied to multiple investigation phases.

Computer Forensics Field Triage Model [13] proposed by M.K. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota is model that aims to cover time-sensitive investigations. This model proposes onsite analysis of evidences, which is opposed to traditional models of seizing all evidences and analysis in laboratory environment.

A common Process Model for Incident Response and Computer Forensics [14] introduced in 2007 by Freiling and Schwittay explicitly introduces *Live Response* element in process model. *Live response* assumes collecting and analysis of evidences from digital sources that are still running. Authors of the model distinct incident response from computer forensics.

Common phases of existing models can be identified as [4]: *Incident detection, Planning, Preparation, Evidence Identification, Evidence Collection, Evidence Transportation, Evidence Analysis, Presentation* and *Conclusion*. Authors in [4] consider that reference principles of *Preserving Evidence*, *Preserving Chain of Evidence* and *Documentation* along with common phases are good basis that should be involved in creating future investigation models.

Recent studies [3] and [4] noted that for proper evaluation of digital investigation model process, interpretation should be considered in frame of Dauberts test. By using this test judges can determine reliability of the digital evidence presented. Five requirements should be followed:

- Whether the theories and techniques employed by scientific expert have been tested;
- Whether the theories and techniques have been under peer review and publication;
- Whether these techniques and theories have a known error rate;
- Whether the existence of relevant standards has been applied to its operation;
- Whether these theories and techniques have been accepted by relevant researchers and community.

According to [3], *Computer Forensics Field Triage Model*, satisfies four out of five requirements. The only requirement considered not satisfied is fifth. Author claims that no evidence exists of its wide acceptance in community.

III. OVERVIEW OF STATE-OF-THE ART CLOUD RELATED FORENSIC INVESTIGATION MODELS AND CHALLENGES

A. Cloud forensic definition

Recent research papers [15]-[21] give brief overview of challenges and establish taxonomy of cloud forensics. In [15] authors give definition of *cloud forensics* as a cross-discipline of *cloud computing* and *digital forensics*. Since *cloud computing* service is based on remote network access, author claim *cloud forensics* as a subset of *network forensics*. NIST in [16] defines it as the application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence.

B. Cloud forensic three-dimensional model

In [19] authors define three-dimensional nature of *cloud forensics*: *Technical, Organizational* and *Legal.*

Technical dimension tends to address technical related issues such as: data collection, live forensics, evidence segregation, virtualized environments and proactive measures. It addresses the problem of segregation of evidences in multiple-tenant nature of cloud environment.

Organizational dimension addresses the issue of determining the participants that are part of investigation. Authors claim that at least two participants are included: cloud service provider and cloud customer. According to authors it becomes difficult to identify participants in case when cloud service providers outsource services to the third parties. This dimension proposes five different roles that are required to establish cloud forensic capability: *Investigators*, *IT Professionals*, *Incident Handlers, Legal Advisors* and *External Advisors*.

Legal dimension addresses issues related to obeying law regulations in different international law zones. It proposes that service level agreements, between customers and cloud service providers, are made in manner that can allow investigators to comply with applicable laws, privacy and security.

C. Cloud forensic challenges

In [18], [19], [20] and [21] authors address technical challenges for *cloud forensic investigation*. Regarding forensic data collection authors find it easier to obtain data of forensic interest for *Infrastructure as a Service* cloud consumers, while on the other side *Software as a Service* cloud services give a little or no access to data. Anyways, forensic investigators working of data copies from *Infrastructure as a Service* cloud services, are not guaranteed to deal with recent copies of disks

and data. Cloud storage providers have encryption enabled on customers data. When encryption is enabled only persons that have encryption keys can deliver unencrypted media. Cloud providers do not offer physical access to storage devices, and customer access to virtual disk devices. Physical access to storage devices can be granted to legal authorities, but that opens the problem of data segregation in multiple-tenant environment. It is hard to secure privacy for tenants not included in investigation.

D. *Cloud forensic investigation state-of-the-art models*

An integrated conceptual digital forensic framework for cloud computing proposed by B. Martini and K. R. Choo [22] consists of four phases:

- Evidence source identification and preservation
- Collection
- Examination and Analysis
- Reporting and presentation

Evidence source identification phase - addresses the issue of cloud service and providers relevant to subject of investigation and proper preservation of acquired data. *Collection phase* - addresses the methods for adequate data capture. It also addresses *chain of custody*. *Examination and Analysis phase* – addresses using well established forensic tools and procedures after all of the data in previous two phases are identified and collected. *Reporting and presentation phase* – addresses well established reporting procedures and presentation of evidences in court of law. The model is proposed as iterative since *Examination and Analysis phase* can lead to identification of new evidence sources.

Digital Forensic Model for a Cloud Environment proposed by M. Sihiya gives *Forensic as a Service* model description. *Cloud Forensic Process Model* as a part of *Forensic as a Service Model* consists of following processes: *Incident Detection, First Response, Planning Process, Preparation, Potential Evidence Identification, Evidence Acquisition, Evidence Transportation, Evidence Storage, Evidence Examination and Analysis, Reporting, Presentation* and *Investigation Closure.* According to noted processes, this model extends [23] by adding nine additional phases. Author gives detailed recommendations regarding to evidence collection, selecting appropriate forensic tools, incident classification, interpretation and industry standards compliance if applicable.

IV. CONCLUSION AND FUTURE WORK

Development of digital forensics procedures and models for cloud forensics application has been established in the past years. Different authors propose models that tend to be more generic and able to apply in wider spectrum of digital investigation processes. Future development of cloud forensics includes not only technical obstacles but rather legal. Cloud providers have data centers on global locations and depending on data center locations, different jurisdictions may apply.

Development of well documented and general digital forensic investigation process model is a challenge that has not been resolved jet. Researchers should focus on continuous cooperation and development of previously established model. Even though if some of the models are widely used, there is no feedback from researchers and forensic investigators. Focusing on feedback papers could help in better understanding of different model applications.

REFERENCES

[1] Palmer et. al., „DTR-T001-01 Technical Report: A Road Map for Digital Forensic Research“, Digital Forensics Workshop (DFRWS), Utica, New York, August 2001

[2] Y. Yosoff, R. Ismail and Z. Hassan, „Common Phases of Computer Forensics Investigation Models“, International Journal of Computer Science & Information Technology, Vol3, No 3, June 2011

[3] R. Montasari, „Review and Assessment of the Existing Digital Forensic Investigation Process Models“, International Journal of Computer Applications, Volume 147-No.7, August 2016

[4] A.Valjarevic, HS Venter, „Analyses of the State-of-the-art Digital Forensic Investigation Process Models“, SATNAC, South Africa 2011

[5] X. Du, N. Le-Khac and M. Scanlon, „Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as Service“,16th European Conference on Cyber Warfare and Security (ECCWS 2017), Dublin, Ireland 2017

[6] K. Mushtaque, K. Ahsan, A. Umer, „Digital Forensic Investigation Models: An Evolution Study“, Journal of Information Systems and Technology Management, Vol. 12- no.2, Sao Paolo, August 2015

[7] M. Reith, C. Carr and G. Gunsch, „An Examination of Digital Forensic Models“, International Journal of Digital Evidence, Volume 1, Issue 3, 2002

[8] B. Carrier, E. Spafford, „Getting Physical with the Digital Investigation Process“, International Journal of Digital Evidence, Volume 2 – No 2, 2003

[9] M.M. Pollitt, „Computer Forensics: An Approach to Evidence in Cyberspace“, Second International Conference on Computer evidence, Baltimore, Maryland, 1995

[10] V. Baryamureeba, F. Tushabe, „The Enhanced Digital Investigation Process Model“, The Digital Forensic Research Conference - DFRWS 2004, USA, Baltimore, August 2004

[11] S. Ciarduhain„ „An Extended Model of Cybercrime Investigations“, International Journal of Digital Evidence, Volume 3, Issue 1, 2004

[12] N. Beebe, J. Clark, „A Hierarchical, Objectives-Based Framework for the Digital Investigations Process“, Digital Investigation, Vol. 2 Issue 2, 2005

[13] M.K. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota, „Computer Forensics Field Triage Process Model“, Proceedings of the conference on Digital Forensics, Security and Law, 2006

[14] C. Freiling, B. Schwittay, „A Common Process Model for Incident Response and Computer Forensics“, 3rd International Conference on IT- Incident Management & IT-Forensics, 2007

[15] S. Simou, C. Kalloniatis, E. Kavakli, „Cloud Forensics Solutions: A Review“, Lecture Notes in Business Information Processing · June 2014

[16] NIST Cloud Computing Forensic Science Working Group, „Draft NISTIR 8006 - NIST Cloud Computing Forensic Science Challenges“, June 2014

[17] G. Sibiya, H. Venter, T. Fogwill, „Digital Forensics in the Cloud: The State of the Art“, IST - Africa 2015 Conference proceedings, 2015

[18] A. Pichan, M. Lazarescu, S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis", Digital investigation Volume 13, June 2015

[19] Ruan K., Carthy J., Kechadi T., Crosbie M. (2011) Cloud Forensics. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics VII. DigitalForensics 2011. IFIP Advances in Information and Communication Technology, vol 361. Springer,

[20] K. Ruan, J. Carthy, T. Kechadi, I. Baggili,"Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results", Digital Investigation Volume 10, Issue 1, June 2013

[21] R. Montasari, "An Overview of Cloud Forensics Strategy: Capabilities, Challenges and Opportunities", Strategic Engineering for Cloud Computing and Big Data Analytics, Springer International Publishing, 2017

[22] B. Martini, K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing", Digital Investigation Volume 9, 2012

[23] M. Sibiya, "Digital Forensic Model for a Cloud Environment", Philosophiae Doctor Thesis, University of Pretoria, February 2015