Cloud Forensic Readiness: Foundations

Lucia De Marco[1,2(✉)], M-Tahar Kechadi[1], and Filomena Ferrucci[2]

[1] School of Computer Science and Informatics,
University College Dublin, Dublin, Ireland
lucia.de-marco@ucdconnect.ie, tahar.kechadi@ucd.ie
[2] Department of Management and Information Technology,
University of Salerno, Fisciano, Italy
fferrucci@unisa.it

Abstract. The advances of the ICT industry in recent years has led to huge popularity of Cloud Computing Services. Due to the fact that the Cloud is distributed and hosts numerous users, its use to commit crimes becomes a critical issue. Proactive cloud forensics becomes a matter of urgency: its capability to collect critical data before crimes happen, thus saving time and energy for the investigations is its primary objective. In this paper, we discuss the basis of Cloud Forensic Readiness, because we believe that such a system is of huge necessity. We begin by carefully defining Digital Forensic Readiness in the Cloud Computing context. We propose a reference architecture for a Cloud Forensic Readiness System (CFRS) together with its features, components, and challenges.

Keywords: Forensic Readiness · Cloud forensics · Cybercrimes · Cyber-Security

1 Introduction

Cloud Computing (CC) is a real evolution in the manner in which information systems are conceived and located. Its main features and opportunities [10] represent the motivations for its rapid diffusion in the last years. Unfortunately, CC currently presents some weak points, which are exploited by criminals, thus leading to serious Cloud incidents [3].

Digital Forensics [12] has evolved through the years, and has been dealing with the collection and management of evidence from several types of devices, from single computers to computer networks and mobile devices. In single machine forensics, the evidence contained within the media are under the control of law enforcement from the time of seizure; in Network Forensics (NF) [12] this remains true, even though the media to consider are both individual machines and network path devices, e.g., routers, access points, switches and server machines. Cloud Forensics (CF) [18] was born from the necessity of managing digital crimes in the architecture of Cloud Computing services.

The paper is structured as follows: Sect. 1 introduces Cloud Computing (CC) and Digital Forensics (DF); in Sect. 2 the Digital Forensic Readiness System

© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2014
P. Gladyshev et al. (Eds.): ICDF2C 2013, LNICST 132, pp. 237–244, 2014.
DOI: 10.1007/978-3-319-14289-0_16

(DFRS) literature review is provided; in Sect. 3 Digital Forensic Readiness (DFR) is introduced and a definition for Forensic Readiness System is provided; in Sect. 4 the architecture for the Cloud Forensic Readiness System (CFRS) is presented, together with its features and challenges; finally, in Sect. 5 we will discuss conclusions and future work.

2 Literature Review

Digital Forensic Readiness focuses on rendering existing computing environments capable of pro-actively collecting and preserving potential digital evidence for later use in digital crime investigations. Several problems arise in this context. One of the constant issues regards the evolving nature of digital forensic investigation procedures; this derives both from the innovations of technological progress and from the skills and techniques adopted by the digital criminals, thus proper techniques for defeating them are necessary. Technical forensic standardization both in industry and academia is missing; in fact, a great variety of customized investigation process models are presented in literature [1,14]. This variety of approaches does not help facilitate the design and implementation of Digital Forensic Readiness Systems (DFRSs). The issues examined in [15] dealt with human, technical, and departmental management problems for implementing a DFRS in large organizations; the proposed solution involved the implementation of frameworks rather than ad-hoc solutions, thus, a novel DFR Management System architecture was proposed and proven by a prototype. Similarly, in [5] the necessity of a structured approach for DFR was presented; it must comply with the legislation and protect the privacy of the users; such an approach seeks to pro-actively configure the existing systems for collecting and preserving the potential evidence; the proposal took into account relevant and established standards and best practices, and considered that the organizations already collected data (though for other purposes), and that they can experience security critical events. Grobler et al. in [7] examined the overlap between Digital Forensics (DF) and Information Security (IS), summarizing that some DF aspects can be considered as IS best practices that miss events prosecution procedures. In the opinion of the authors a DFRS can enrich the security strategies of an organization; its main feature is providing a way to prepare the existing system for an incident by collecting digital evidence and minimizing the cost of investigations. Thus, DFR will become a component of the IS best practices, demonstrating that protecting valuable company information resources is critical [6].

3 Forensic Readiness

Some Digital Forensic Readiness advantages were investigated in literature; an important milestone is the set of guidelines presented by Rowlingson in [16], designed to facilitate the implementation of a DFRS; this work places emphasis on the features that a DFRS must respect to be effective. Again, the impact of

DFR in a corporate context was analysed in [13], where some positive aspects were highlighted, e.g., the help for enhancing the security strategy of an organization, the reduction of security incidents, the availability of evidence, and the derived effectiveness of an investigation. Finally, another DFRS proposal involves Wireless Sensors Networks [8], where a forensic readiness prototype was conceived as an additional layer that does not modify the original architecture of an existing IEEE 802.15.4 network.

3.1 Definition

DFR was defined in [16,19] as "the ability of an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation", but we consider it as one of the features of a DFRS to achieve a certain aim. To the best of our knowledge, DFR means implementing an information system capable of recording the potential evidence for the investigations, encrypting and storing them for being accessed after a crime happens. We define DFR as *"an Information System implemented into another system architecture with the aim of collecting and monitoring sensitive and critical information related to digital crimes before they happen, leading to save time and money for the investigations. The data is closely related to the system artifacts and logging tools available at the moment. The data is then encrypted in order to guarantee more protection and, eventually, stored on a third party server that will act as a safe, only accessible to selected subjects".* This definition is considered general and adaptable to every computing context, thus we can affirm that it is valid both for the past and the future, as well as for CC.

4 Cloud Forensic Readiness

The main purpose of this paper is to provide a reference architecture for a Cloud Forensic Readiness System (CFRS) by designing it. The potential evidence collected by a DFRS have the same utility of CCTV recordings: preventively saved and when necessary accessed. This facility must be given to Cloud Computing, because, due to its huge popularity, it is also object of several attacks, thus a way to conduct forensic investigations effectively, e.g., saving time, money and resources, must be designed. In a recent survey [17] almost the 90 % of the interviewees, who were familiar with digital forensics, stated that "a procedure and a set of toolkits to proactively collect forensic-relevant data in the cloud is important". For a Cloud Forensic Readiness System, we believe that an accurate definition and model must be provided, in order to clarify the tasks, the activities and the stakeholders to consider.

4.1 Technical Challenges

Cloud Computing architecture unfortunately presents several technical challenges related to Forensic Readiness [2]; no standard is present, and no structured

manner to perform an investigation has yet been defined. CC obfuscates physical access to the servers, leading users and data owners to be unaware of the physical location of the machines on which their data is stored, and creating uncertainty regarding the provenance of data and processes. Furthermore, the logs from network components are impossible to retrieve, because no routing information is available. Some digital evidence sources are missing, such as the customer's browser logs, which could provide a great deal of clues to reconstruct a case timeline; also the synchronization of timestamps is necessary for a correct case timeline reconstruction, as affirmed also in [17]. Moreover, due to the fact that logs and encryption processes running on virtual machines (VMs) can be controlled by malicious or corrupted hypervisors, an open challenge concerned with determining how a VM can be protected by compromised VM Monitors. Furthermore, defining both a procedure and a set of tool-kits for recording and maintaining a Chain of Custody (CoC) [9] into the Cloud investigations is a challenge to be addressed. Another technical challenge is related to the variety of log formats to be investigated. Finally, because the current international legal structure is far away from managing data segmented and duplicated all over the world, a CFRS must also manage the multiple jurisdictions issue.

4.2 CFRS Reference Architecture

The proposed CFRS will be implemented into a Cloud Computing architecture without modifying its structure, as well as done in [8]. The proposed reference architecture is composed of several subsystems, as illustrated in Fig. 1, which need to communicate and exchange data with each other. The OVF standard language [11] is suitable for the creation of communication channels: OVF is capable of creating and distributing software applications to be executed on VMs, independently from hypervisors and from CPUs architectures; it exploits the XML standard to establish the configuration and the installation parameters, and it can be extended for future hypervisor developments. In our system, an OVF module between the CC architecture and the CFRS components is necessary: it will convert the Cloud data formats into a new defined and appropriate XML one, in order to render readable and usable the necessary information by the several system components, listed in Fig. 1.

– Monitored Data: includes CC common features and tools [4] involving monitored information, which are: Database and File Activity Monitoring, URL Filtering, Data Loss Prevention, Digital Rights Management, and Content Discovery. The Database and File Activity Monitoring tools are capable of recognizing whenever a huge amount of data is pushed into the Cloud or replicated, thus indicating a data migration; the Data Loss Prevention facility is used for monitoring data in motion; it also manages policies and rights. URL Filtering controls the customer's connections to the Cloud Services, thus it can be useful during the construction of a case timeline. Finally, we can integrate the Digital Rights Management System and the Content Discovery System, where the former is responsible for implementing and monitoring the

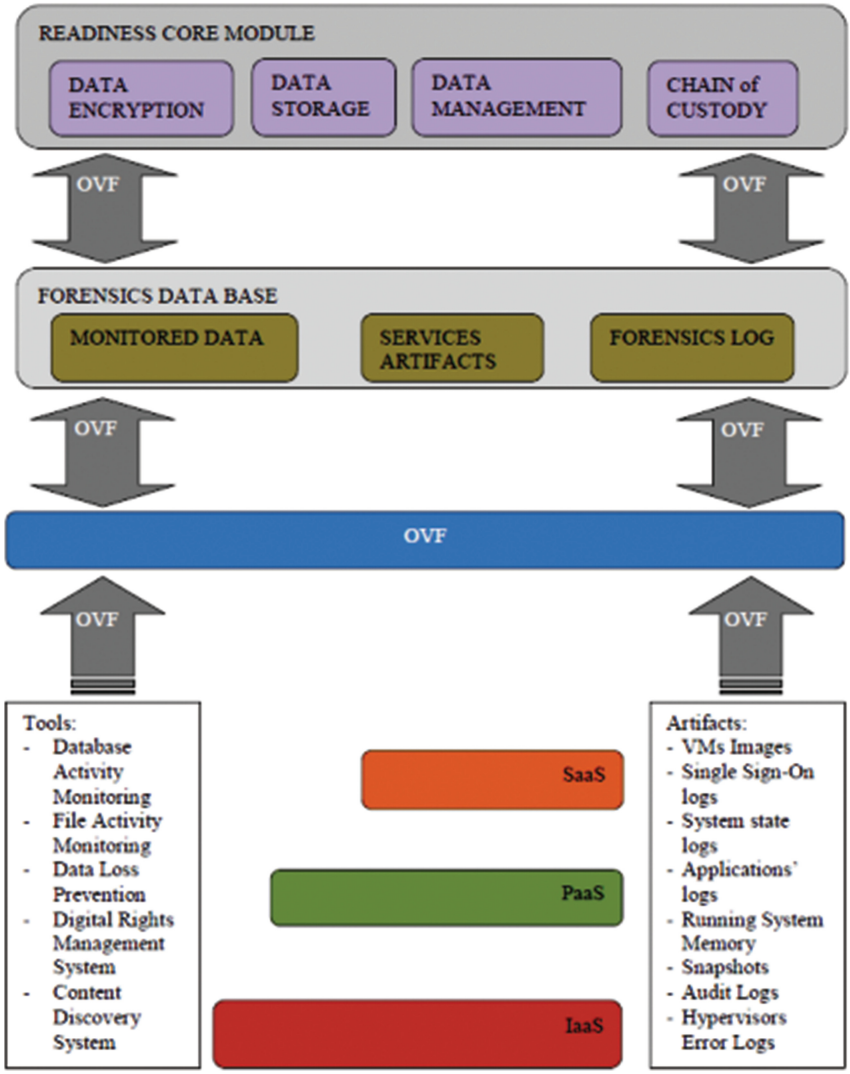

Fig. 1. CFRS reference architecture

customers' rights and restrictions on data, as stated by the SLA's clauses and terms of use contracts co-signed by CSPs and customers; the latter includes tools and processes aimed to identify sensitive information in storage, allowing us to define policies for them and to identify their violations;

– Services Artifacts: this component includes a significant quantity of CSPs artifacts, i.e., from SaaS clouds, the VM images and the Single Sign-On logs; from PaaS clouds, the system states and applications logs; and from IaaS clouds, the snapshots and the running system memory;

- Forensic Log: this module collects suitable logs, and they are: audit logs from Cloud Auditors; and error logs coming from hypervisors indicating problematic events. Both of them are relevant for incident response;
- Readiness Core Module: this module is dedicated to the computation of the data collected in the previously listed system modules, i.e., the Monitored Data, the Service Artifacts, and the Forensic Logs. We can affirm that the Core module contains all the functional requirements of the readiness system, e.g., data encryption, data storage, and data management for the purpose of events timeline reconstruction, and Chain of Custody report. All these submodules represent a dedicated functional requirement.

4.3 Usage of CFRS

In order to obtain the most from the proposed system, some recommendations must be respected. The CC must provide the necessary features for monitoring by the CFRS described above. As mentioned above, the Cloud artifacts used by the system are common Cloud features [4], therefore their presence at the moment of the system installation must be verified. They are essentially the following:

- Components dedicated to the monitoring of both databases and files, necessary for detecting data migrations.
- Features for filtering URLs, aimed to verifying the connections made.
- Tools with the purpose of controlling policies and rights established by the SLAs, Contracts, and Terms of Use, and possibly capable of creating new ones for sensitive data.

The same importance, even more, is assigned to the potential evidence data sources; this encompasses several logs types, for which logging facilities are already present; likewise snapshots, for which running system memory image tools are necessary. From all these premises, the installation and the usage of a CFRS is very important for accomplishing distinct aims. Implicitly, the first aim is rendering the Cloud environment ready for digital forensics, by executing the functionalities included into the Readiness Core Module; hence, data encryption functions have to be executed; the data are stored in a dedicated environment, which has to be physically prepared; the aim of reconstructing the case timeline and establishing the chain of custody [9] in case an incident occurs. The system's added value is in the provision of more control over data, on the access to services, and on the usage rules and constraints.

5 Conclusions and Future Work

The principal aim of this paper is to provide the basis for Cloud Forensic Readiness; its main contribution involves two distinct proposals; with the first proposal, we attempted to clarify what must be intended for Digital Forensic Readiness: we provided a definition adaptable to several different computing

environments; with the second proposal, we proposed a CFRS reference architecture in order to corroborate our research work direction. We presented a proposal that must be considered a greenfield software engineering product, because there is no similar proposal in literature. At the same time, our proposal both takes advantage of several CC aspects specified by the Cloud Security Alliance, common to various CSPs, and integrates them in specific system components that implement dedicated functions. In the future, we will continue our research in this and we will provide more details about the CFRS reference architecture, for the purpose of prototyping it.

References

1. Alharbi, S., Weber-Jahnke, J., Traore, I.: The proactive and reactive digital forensics investigation process: a systematic literature review. In: Kim, T., Adeli, H., Robles, R.J., Balitanas, M. (eds.) ISA 2011. CCIS, vol. 200, pp. 87–100. Springer, Heidelberg (2011)
2. Birk, D.: Technical challenges of forensic investigations in cloud computing environments. In: Workshop on Cryptography and Security in Clouds, pp. 1–6 (2011)
3. Choo, K.K.R.: Cloud computing: challenges and future directions. Trends Issues Crime Crim. Justice **400**, 1–6 (2010)
4. Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing (2011)
5. Danielsson, J., Tjostheim, I.: The need for a structured approach to digital forensics readiness. In: IADIS International Conference e - Commerce (2004)
6. Endicott-Povsky, B., Frinckle, D.A.: A theoretical framework for organizational network forensic readiness. J. Comput. **2**(3), 1–11 (2007)
7. Grobler, C.P., Louwrens, C.P.: Digital forensic readiness as a component of information security best practice. In: Venter, H., Elofif, M., Labuschagne, L., Elofif, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 13–24. Springer, Boston (2007)
8. Mouton, F., Venter, H.S.: A prototype for achieving digital forensic readiness on wireless sensor networks. In: AFRICON, pp. 1–6 (2011)
9. National Institute of Justice: Electronic Crime Scene Investigation: A Guide for First Responders (2008)
10. National Institute of Standards and Technology: NIST Definition of cloud computing v15. NIST Editor. Gaithersburg, MD (2009)
11. Open Virtualization Format: OVF Standard. http://www.dmtf.org/standards/ovf
12. Palmer, G.: A road map for digital forensics research. In: Report From the First Digital Forensics Research Workshop (2001)
13. Pangalos, G., Ilioudis, C., Pagkalos, I.: The importance of corporate forensic readiness in the information security framework. In: 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), pp. 12–16 (2010)
14. Pollitt, M.: An ad hoc review of digital forensic models. In: Second International Workshop on Systematic Approaches to Digital Forensic Engineering, pp. 43–54 (2007)
15. Reddy, K., Venter, H.S.: The architecture of a digital forensic readiness management system. Comput. Secur. **32**, 73–89 (2013). ISSN: 0167-4048

16. Rowlingson, R.: A ten step process for forensic readiness. Int. J. Digital Evid. **2**(3), 1–28 (2004)
17. Ruan, K., Baggili, I., Carthy, J., Kechadi, T.: Survey on cloud forensics and critical criteria for cloud forensic capability: a preliminary analysis. In: Proceedings of the 6th Annual Conference on Digital Forensics, Security and Law (2011)
18. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M: Cloud forensics: an overview. In: IFIP International Conference on Digital Forensics, vol. 7 (2011)
19. Tan, J.: Forensic Readiness. @Stake, Cambridge (2001)