Forensic Process as a Service (FPaaS) for Cloud Computing

Amna Eleyan
Computing Department
Manchester Metropolitan University
Manchester, UK
a.eleyan@mmu.ac.uk

Derar Eleyan
Computer Science Department
Palestinian Technical University
Tulkarem, Palestine
d.eleyan@ptuk.edu.ps

Abstract— Cloud computing is the technology that enables individuals and businesses to utilize computing services (e.g. online file storage, social networking sites, webmail)and a shared pool of resources (e.g. data storage space, networks, user applications) from anywhere over the Internet. Cloud computing has become popular as a cost-effective and convenient computing paradigm. However, cloud computing architecture is at its infancy stage and lacks support for security and forensic investigations. Due to the distributed and virtual nature of cloud, malicious activities can be carried out very easily and are very difficult to subsequently investigate. Cloud forensic investigators currently face challenges as they lack forensic tools and techniques in context of cloud. This highlights the need to develop the new research area of digital forensics in the cloud computing model.

This paper presents a cloud forensic process that consists of (i) Identification, (ii) Collection/Acquisition and preservation, (iii) Examination/Processing and analysis, and (iv) Results dissemination phases. In addition, this paper develops the proposed forensic process as a service (FPaaS) using cloud-based Business Process Execution Language (BPEL) that combines the four phases/services into a new composite service called FPaaS.

Keywords—cloud computing; cloud forensics; forensic process; business process execution language (BPEL)

I. INTRODUCTION

A. Motivation

Cloud computing is a computing paradigm that provides on demand computing resources on pay-as-you-use basis. In recent years, cloud computing technology is getting popular in private industries and in government sectors [1], [2]. This is because this technology is cost effective and no additional cost is required for physical and administrative infrastructure.

Clouds use virtualization and a multi-tenant usage model to utilize its resources. However, this paradigm makes malicious activities and attacks on clouds difficult to prevent and investigate. To investigate cloud-based crimes, investigators have to conduct a digital forensic investigation in the cloud environment. This new area in the field of digital forensic is known as *Cloud Forensics* [3].

Digital forensics has increased rapidly and new techniques have been developed. Unfortunately, many of the tools of digital forensics are not valid in context of cloud. For example, in a cloud environment, investigators cannot physically access the evidence as in traditional locally hosted computing system. Therefore, cloud forensics brings new challenges from both technical and legal point of view and has opened new research area for security and forensic researchers.

B. Related Work and Contribution

Researchers and forensic practitioners have proposed several digital forensic process models and frameworks. Martin and Choo [4] present an integrated conceptual digital forensic framework for cloud computing that consists of (i) Evidence source identification and preservation, (ii) Collection, (iii) Examination and presentation, and (iv) Reporting and presentation phases. In the proposed framework, phase (iii) iterates back to phase (i) if more data or evidence is required.

Pichan et al. [5] present digital forensic model for cloud computing that consists of (i) Identification, (ii) Preservation, (iii) Collection or acquisition, (iv) Examination and analysis, and (v) Reporting and presentation. Pichan et al. describes the sub process activities, the challenges and recommended solution in each phase of the process.

Zawoad et al. [3] propose computer forensics process that consists of (i) Identification, (ii) Collection, (iii) Organization, and (iv) Presentation. This paper explores the cloud forensic challenges and issues in each phase of the proposed process.

Kent et al. [6] present National Institute of Standards and Technology (NIST) forensic model consisting of (i) Collection, (ii) Examination, (iii) Analysis and reporting phases.

McKemmish [7] presents forensic computing model that consists of (i) Identification, (ii) Presentation, (iii) Analysis, and (iv) Presentation phases.

Shan and Malik [8] propose digital forensic framework for cloud that consists of (i) Identification, (ii) Data Collection and preservation, (iii) Analysis and presentation phases. The authors illustrate the challenges and suggested solutions in each phase of the framework.

Quick and Choo [9] propose a digital forensic analysis cycle and iterative model that consists of (i) Commence, (ii) Prepare and respond, (iii) Identify and collect, (iv) Preserve, (v) Analyse, (vi) Present, (vii) Feedback, and (viii) Complete. This paper proposes forensic process that consists of (i) Identification, (ii) Collection/Acquisition and preservation, (iii) Examination/Processing and analysis and (iv) Results dissemination phases.

The proposed forensic process combines the three forensic frameworks of Pichan et al. [5], Martin and Choo [4], and Shah and Malik [8] to improve forensic investigation in a cloud environment. Although the names and purposes of the phases in our forensic process are similar to Pichan et al. [5], Martin and Choo [4], and Shah and Malik [8], the flow of the process undertaken in each phase is somewhat different. For example, in phase (ii), the two steps Collection and preservation are combined together in one phase, similar to Shah and Malik [8]. In addition, the flow of the process conducts the collection step first then the preservation step. Whereas in Pichan et al. [5], Martin and Choo [4], the collection and preservation steps are conducted in different phases starting with preservation phase then afterward collection phase. Furthermore, the iteration back from phase (iii) Examination and analysis to phase (i) Identification is similar to Martin and Choo [4]. In addition, this paper develops a forensic process as a service (FPaaS) using cloud-based BPEL that combines the four phases/services (identification, collection and preservation, examination and analysis, and results dissemination) into a new composite service called FPaaS.

II. Background

A. Cloud Computing

NIST [10] defines cloud computing as " a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."

There are three main cloud service models [10]:

- *Software as a Service (SaaS)*. The consumer can use software applications that are provided by a cloud service provider (CSP). Google Apps [11] is an example of SaaS.
- *Platform as a Service (PaaS)*. This model provides an application programming interface (API) for customers to create and host their applications. Google App Engine [12] is an example of PaaS.
- *Infrastructure as a Service (IaaS)*. This model allows customers to lease infrastructure such as processing power, volatile memory and disk based storage to host virtual machines and they can run any software they select. An example of IaaS is Amazon EC2 [13].

B. Cloud Forensics

The NIST Cloud Computing Forensic Science Working Group proposed the following definition of cloud forensic [14]: "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.". Ruan et al. [15] identify three dimensions in cloud forensics: technical, organizational and legal.

The procedures of cloud forensics depend on the service and deployment model of cloud. In IaaS, customers have more control over data acquisition and investigation process than SaaS and PaaS and mostly depend on the CSP to collect the digital evidence. From SaaS and PaaS models, the customers have control over the applications and can get a high level of logging information that facilitates the investigation procedure [3]. Figure 1 illustrates the customers' control over different layers in SaaS, PaaS and IaaS models.

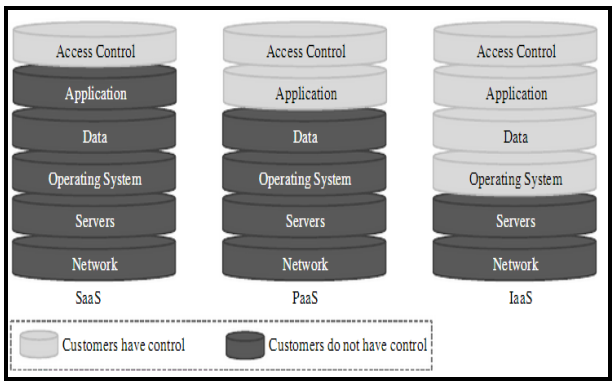

Fig. 1. Customers' control in different service model [3].

III. Cloud Forensic Process

This section describes the proposed cloud forensic process. Figure 2 illustrates the proposed process, which consists of (i) Identification, (ii) Collection/Acquisition and preservation, (iii) Examination/Processing and analysis and (iv) Results dissemination phases. These phases are described below.

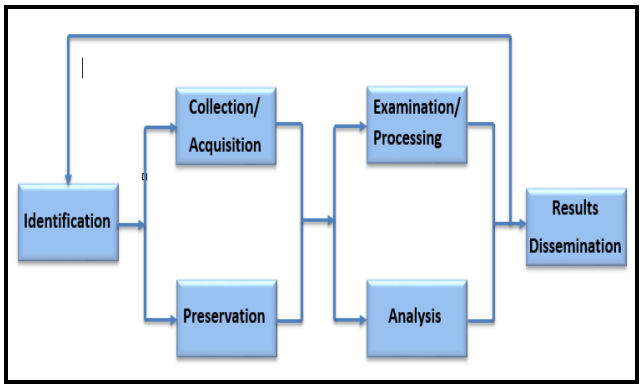

Fig. 2. Cloud forensic process

1. Identification

Identification is reporting misuse of cloud or malicious activity such as deleting files, illegal use of storing files and so on [8]. The forensic process begins with identifying the digital evidence. The evidence in a cloud could be the image of virtual machines, files stored in cloud servers and logs from cloud service providers (CSP). The identification process consists of two steps as in [5] [3]: the incident identification and the evidence identification. The incident identification is reporting of malicious activity from customer, organization or Cloud service provider (CSP). This step requires identifying all the machines and file systems, which are likely contain the related evidence. Evidence identification step is about the digital artefact that should be presented in the court. This step requires identification of the evidence in the media such as cloud servers, mobile devices and network devices.

2. *Collection/Acquisition and Preservation*

The data collection and acquisition is a crucial phase of forensic procedure. Any errors that may occur will affect the whole investigation process. Due to ephemeral nature of cloud computing and the physical inaccessibility of evidence artefacts makes the evidence collection procedure difficult in the cloud environment. In addition, physical seizure of all the servers in a cloud computing may be impossible due to the amount of hardware involved, the multi-tenancy or the data being physically located in another jurisdiction [4]. The data collection phase should also consider the preservation phase for collecting evidence.

Preservation is the protection the protection of the integrity of the evidence throughout the investigation process [16]. The evidence preservation is a continuous process until the evidence is presented in court. Therefore, the evidence's integrity should be maintained and ensure the originality of the data throughout the investigation lifecycle [5].

2. Examination/Processing and Analysis

Examination and analysis phase comes after collecting the digital evidence and preserving it. Examination is defined as "Forensic tools and techniques appropriate to the types of data that were collected are executed to identify and extract the relevant information from the collected data while protecting its integrity" [6].

If the evidence extracted from the analysis phase may not be admissible or inadequate in a court of law, then the process should go back to the first phase, which is the evidence identification and then go through the process again.

3. Results Dissemination

This phase consists of report findings step and presentation findings step. Digital evidence and analytical reports are presented to the court in this phase. NIST defined Reporting as a process which "includes describing the actions performed, determining what other actions need to be performed, and recommending improvements to policies, guidelines, procedures, tools, and other aspects of the forensic process" [6]. The report should include information on all processes, the tools and applications.

IV. Forensic Process as a Service (FPaaS) Using Business Process Execution Language (BPEL)

Business Process Execution Language (BPEL) is an XML-based language for specifying actions and executions of business processes within Web services technology. BPEL is a top-down approach of Service Oriented Architecture (SOA) through composition, orchestration and coordination of Web services. By using BPEL, several Web services can compose easily into new composite service called business process [17].

In this section, a forensic process is created using cloud-based BPEL that combines the four phases (identification, collection/acquisition and preservation, examination/processing and analysis, and results dissemination) of the proposed forensic process (see section III) into a complex forensic process. Each phase is considered as a service and the four phases/services are integrated together using BPEL to define a complex forensic process or service. The proposed composite forensic process/service will deploy on the cloud as a service, which is called forensic process as a service (FPaaS). FPaaS is supposed to be orchestrated by a BPEL specification and executed by a BPEL execution engine.

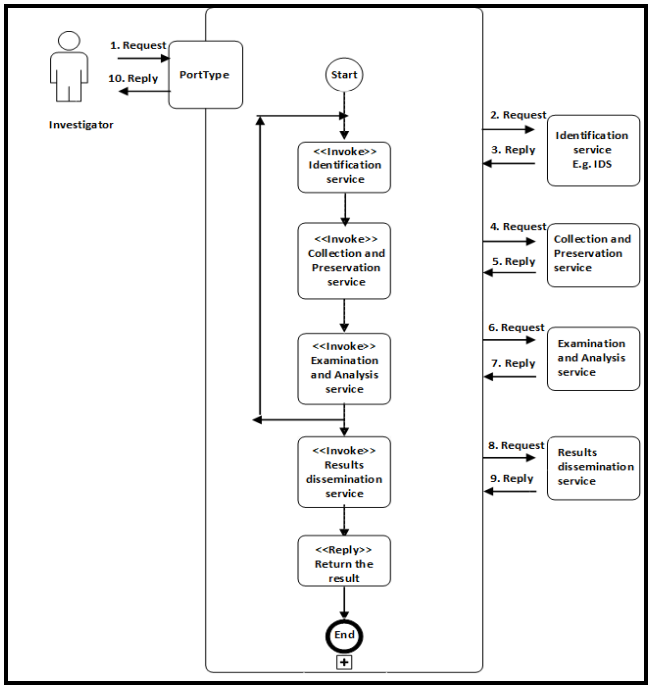

Fig. 3. The proposed forensic process as a service (FPaaS)

Figure 3 illustrates the forensic process as a Web service. The investigator send a request to invoke FPaaS service. This service is a complex business process, which combines four Web services: Identification service, Collection and preservation service, Examination and analysis service and Results dissemination service.

FPaaS can be deployed to the three service models as described below [18]:

IaaS

In IaaS service model, customers have full control over operating system, the middleware and the applications as shown in Figure 4. BPEL Installation through IaaS model is similar to the traditional on-premise model. Customer can install operating systems, middleware and applications.However, customer has to secure the system from attackers such as blocking ports, running an anti-virus software and enforcing access control policies [18].

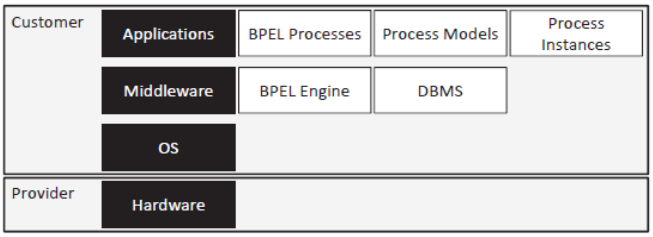

Fig. 4. Providing BPEL through IaaS [18]

PaaS

Figure 5 illustrates that PaaS providers host hardware, operating system and platform middleware such as a BPEL engine and a database management system (DBMS). The execution engine is part of the platform. The engine can be used by multiple users as the platform is shared. Customer no longer can control the data storage and management, which leads to security issues [18].

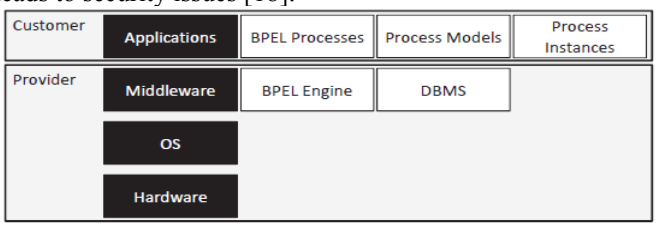

Fig. 5. Providing BPEL through PaaS [18]

SaaS

Figure 6 illustrates that the cloud provider is responsible for the application. The process is no longer visible to the customers. The application can be provided to customers as single-tenant or multi-tenant model. In a single-tenant, one BPEL engine and DBMS is installed for each process. Whereas, in a multi-tenant, single BPEL engine and DBMS is installed for multiple customers and multiple business processes. The storage data should be protected against unintended access by the SaaS providers or other customers [18].

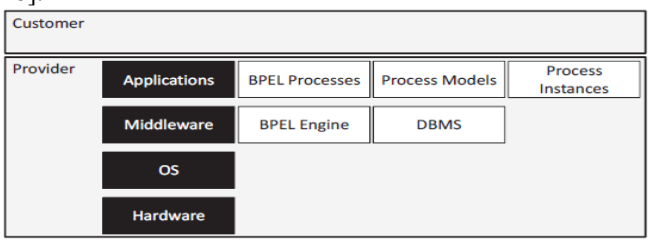

Fig. 6. Providing BPEL through SaaS [18]

V. Conclusion and Future Work

The virtual nature of cloud computing is pushing digital forensics into a new horizon. Many challenges are existing in the cloud including jurisdictional and technical issues. This paper proposes forensic process that consists of four phases: Identification, Collection and acquisition, Examination and analysis and result dissemination. This paper presents a conceptual model of forensic process as a service (FPaaS) using cloud-based BPEL. Further works are required to develop each service in the forensic process and implement FPaaS.

References

[1] H. Clancy, "Microsoft data suggests SMB cloud adoption poised to double," 2012. [Online]. Available: http://www.zdnet.com/article/microsoft-data-suggests-smb-cloud-adoption-poised-to-double/. [Accessed 13th May 2015].

[2] S. Paquette, P. T. Jaeger and S. C. Wilson, "Identifying the security risks associated with governmental use of cloud computing," Government Information Quarterly, vol. 27, no. 3, pp. 245-253, 2010.

[3] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," arXiv, vol. 1, 2013.

[4] B. Martini and K.-K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing," Digital Investigation, vol. 9, pp. 71-80, 2012.

[5] A. Pichan, M. Lazarescu and S. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis," Digital Investigation, vol. 13, pp. 38-57, 2015.

[6] K. Kent, S. Chevalier, T. Grance and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST, 2006.

[7] R. McKemmish, "What is Forensic Computing?," Australian Institute of Criminology, 1999.

[8] J. Shah and L.G.Malik, "An Approach towards Digital Forensic Framework for Cloud," in IEEE International Advance Computing Conference (IACC), 2014.

[9] D. Quick and K.-K. R. Choo, "Digital droplets: Microsoft SkyDrive forensic data remnants," Future Generation Computer Systems archive, vol. 29, no. 6, pp. 1378-1394, 2013.

[10] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2011.

[11] Google, "Google Apps for Work," Google, [Online]. Available: https://www.google.com/work/apps/business/products/. [Accessed 20 May 2015].

[12] Google, "Google Cloud Platform," [Online]. Available: https://cloud.google.com/appengine/docs. [Accessed 20 May 2015].

[13] Amazon, "Amazon Elastic Compute Cloud," [Online]. Available: http://aws.amazon.com/ec2. [Accessed 20 May 2015].

[14] NIST Cloud Computing Forensic Science Working Group, "NIST Cloud Computing Forensic Science Challenges," NIST , 2014.

[15] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, "Cloud forensics: An overview," in 7th IFIP Int. Conf. Digital Forensics , 2011.

[16] Y. Lei and Y. Cui, "Research on Live Forensics in Cloud Environment," in 2nd International Symposium on Computer, Communication, Control and Automation (3CA), 2013.

[17] M. Juric, B. Mathew and P. Sarang, Business Process Execution Language for Web Services : BPEL and BPEL4WS, Birmingham: Packt, 2004.

[18] T. Anstett, F. Leymann, R. Mietzner and S. Strauch, "Towards BPEL in the Cloud: Exploiting Different Delivery Models for the Execution of Business Processes," in Congress on Services-I, Washington, 2009.