Software Agent and Cloud Forensics: A Conceptual Framework

Arwa Ibrahim Ahmed
Information Systems Department
Princess Nourah Bint Abdulrahman University (PNU),
Riyadh, Kingdom of Saudi Arabia (KSA)
Email: Ariahmed@pnu.edu.sa

Abstract: - Recently, a number of digital storage and services of computing data is moving towards cloud computing. Due to this movement, in case of attack occur in the cloud this would like more investigation and acquiring. Digital forensics is the application of science to the identification, examination, collection, and analysis of data while preserving the information and maintaining a strict chain of custody for the data. Cloud forensics is the application of digital forensics in cloud computing. In this paper a framework is acquiring the digital forensics for cloud computing is proposed. A framework consists of two main layers, firstly, cloud forensics layer that consists of Cloud Service Provider (CSP), law enforcement, forensics investigators and cloud users. Secondly, Multi Agent System (MAS) architecture layer that consists of two main agents: Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA) are proposed. Our results in the practical scenario defined formally in this paper, show the Round Trip Time (RTT) for an agent to acquire the cloud forensics and measured by the times required for an agent to travel around different number of CSPs before and after the implementation.

Key-Words: - Cloud Computing, Cloud Service Provider, Cloud Service Agreement, Digital Forensics, Cloud Forensics and Multi Agent System.

1 Introduction

Nowadays, cloud computing has grants several promising technological, services and economic opportunities that have a prospective to become an evolutionary point in the new era of computing environment [1]. Cloud computing can be defined as “a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLAs) established through negotiation between the CSP and cloud users” [2].

SLAs measure the service provider’s performance and quality in a number of ways. Some metrics that SLAs may specify include:

- Availability and uptime -- the percentage of the time services will be available
- The number of concurrent users that can be served
- Specific performance benchmarks to which actual performance will be periodically compared
- Application response time
- The schedule for notification in advance of network changes that may affect users
- Help desk response time for various classes of problems
- Usage statistics that will be provided.

According to Pollit and Whiteledge [3], digital forensics is the science of collecting, preserving, examining, analyzing and presenting relevant digital evidence for use in judicial proceedings. Digital forensics is no longer associated only to a laboratory in police and security agencies, but it is also used outside that area. The most digital forensics risks are judicial proceedings. Thus it must have a correct procedure in conducting the forensic investigation and doing the inspection setup where this procedure or methodology must basically base on the scientific principles [4].

Cloud forensics is a cross discipline of cloud computing and digital forensics. Cloud computing is a shared collection of configurable network resources (e.g., networks, servers, storage, applications and services) that can be reconfigured quickly with minimal effort [5]. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law [6].Cloud forensics is a subset of network forensics. Network forensics deals with forensic investigations of networks. Cloud computing is based on broad network access. Therefore, cloud forensics follows the main phases of network forensics with techniques tailored to cloud computing environment.

Multi Agent System is a technique in the artificial intelligence area focusing on the system where several agents communicate with each other through the Agent Communication Agent (ACL) [7]. According to Durfee et al., [8], MAS is defined as “a loosely coupled network of problem-solver entities that work together to find answers to problems that are beyond the individual capabilities or knowledge of each entity”.

Agents must be able to interact to achieve goals. Agents may exhibit different types of behaviors when interact with each others such as selfish or benevolent behavior. In cloud forensics scenarios, selfish agents ask for help from other agents if they are overloaded and never offer help such as the agent that serving cloud data acquisitions service never help other agents for the same service [9]. Benevolent agents always provide help to other agents because they consider system benefit is the priority such as the agent that serving forensics law enforcement for CSPs service are always ready to help other agents to complete their tasks [9].

The issue of digital forensics in cloud requires fundamentally different tools, techniques and training [10] [11]. Therefore in this paper a framework will acquiring the digital forensics for cloud computing is proposed. The main contributions of this paper are, firstly, we identify the technical scenario of a crossing discipline of digital forensics and cloud computing, secondly, we propose a digital cloud framework based on MAS architecture that assist in applying cloud forensics application to the CSPs.

The rest of the paper is organized as follows: section II reviews previous and related work. Section III presents the proposed cloud forensics framework and its MAS architecture. Section IV illustrates the MAS architecture design using Prometheus Methodology. Section V presents a case study. The result and discussion of the work presents in section VI. Section VII concludes the work.

2 Related works

Multiple toolkits for developing agents have been implemented. [12][13][14] With understanding of points covered by above works, it’s possible to head forth for prototyping intelligent agent system targeting the cloud forensics data. In cloud forensics, clouds’ forensics requires Intelligent Systems owing to the voluminous data content within the data store of the CSP. The functional programming that dominates data center data processing is observed [15].

According to Birk, digital forensics evidence can be available in three different states in cloud – at rest, in motion, and in execution [16].

According to Shams and Ragib [17], Cloud forensics procedures will vary according to the service and deployment model of cloud computing. For (Software as a Service) SaaS and (Platform as a Service) PaaS, they have very limited control over process or network monitoring. Whereas, they can gain more control in IaaS and can deploy some forensic friendly logging mechanism. The first three steps of computer forensics will vary for different services and deployment models. For example, the collection procedure of SaaS and IaaS will not be same. For SaaS, they solely depend on the CSP to get the application log, while in IaaS, they can acquire the Virtual machine instance from the customer and can enter into examination and analysis phase. On the other hand, in the private deployment model, they have physical access to the digital evidence, but they merely can get physical access to the public deployment model.

Several researchers have pointed out that evidence acquisition is a forefront issue with cloud forensics [18] [19]. Ruan et al. [18] suggested that evidence collection should obey “clearly-defined segregation of duties between client and provider,” though it was unclear who should collect volatile and non-volatile cloud data and how. Taylor et al. [19] also lamented about the lack of appropriate tools for data from the cloud, noting that “Many of these tools are standardized for today’s computing environment, such as EnCase or the Forensics Tool Kit [sic].”

NIST currently publishes a Digital Data Acquisition Tool Specification, which “defines requirements for digital media acquisition tools in computer forensic investigations” [20]. The most recent version of the specification was written in 2004, before cloud computing (as currently defined) was known to exist then.

3 proposed cloud forensics framework and its mas architecture

A. Proposed Cloud Forensics Framework:

Fig. 1 shows a schematic representation of proposed cloud forensics framework. The framework has been built using two layers.

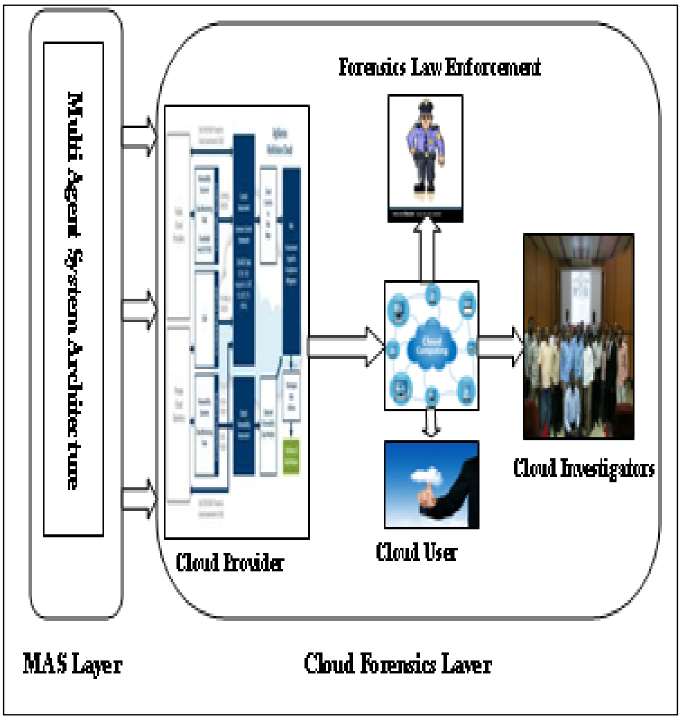

Fig.1. Proposed Cloud Forensics Framework

The functionality of those layers can be summarized as follows:

Multi Agent System (MAS) layer:

This layer has two agents: the Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA). CAA acts as an effective bridge between the CSPs and the rest of the agents.

Cloud Forensics layer:

Cloud data storage has four different network entities can be identified as follows:

- Cloud Service Provider (CSP): a CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems [9].
- Cloud Forensics law enforcement: The use or application of scientific knowledge to a point of law, especially as it applies to the investigation of crime in cloud computing.
- Cloud Forensics investigator: Public and private sectors who investigate the cloud forensics such as a researchers, lawyers, cloud experts and cloud companies.
- Cloud user: who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations [9].

B. Proposed MAS Architecture

In MAS architecture, we proposed two types of agents: Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA). The scenarios of the agents are summarized as follow:

a) Cloud Acquiring Agent (CAA):

In CAA scenario depicted by Fig. 2, the simplest scenario for CAA interaction is provided. In a service offering there is a single relation between the cloud user and the CSP, where the CSP may or may not provide services via a cloud carrier. The cloud user signs an SLA (SLA1) with the provider. The CSP signs a separate Service Level Agreement (SLA2) with the carrier when the relation between carrier and the CSP exist. A cloud auditor may be involved to audit SLA(s). Forensic segregation of duties, requirements and implementations need to be defined and audited through the SLA(s). An internal investigation exists when the user and the provider shared systems. An external investigation is initiated by law enforcement towards the cloud user, CSP or to external assistance in enhancing forensic capabilities in facing in internal or external investigations. Forensic artifacts are scattered between the cloud user and producer systems.

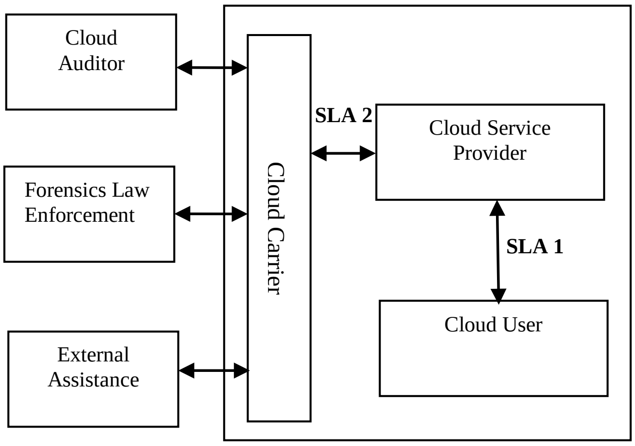

Fig 2. Cloud Acquiring Agent Scenario

b) Cloud Forensics Agent (FCA):

In FCA scenario depicted by Fig. 3, the cloud broker is acting as a CSP to the cloud user. The cloud user signs an SLA A with the FCA. The FCA signs a range of SLAs (SLA B1, SLA B2, SLA B3 and so on) with multiple CSPs, and may sign a separate SLA, SLAC with a cloud carrier when services are delivered through the carrier

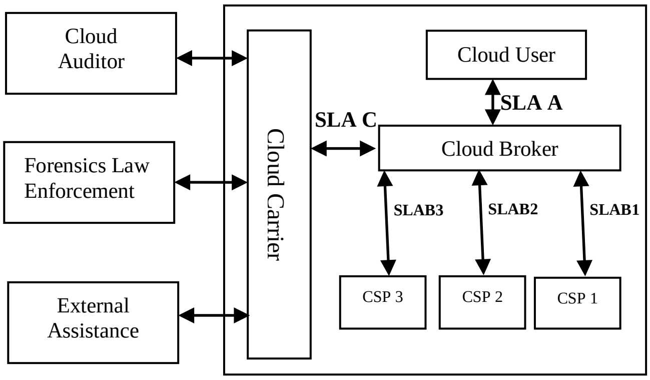

Fig 3. Cloud Forensics Agent Scenario

3.1 MAS architecture design

To ensure that the proposed MAS architecture has meet it objective in cloud forensics, hence the MAS architecture is therefore designed.

MAS architecture design shall be specified to determine the types of agents, events, protocols and agent capabilities, using the Prometheus methodology [21]. The sections below go through each of Prometheus' three phases in more detail and will discuss the notations used by the methodology as well as some specific techniques.

The Prometheus methodology consists of three phases:

- System Specification: where the system is specified using goals (illustrated in Fig. 4.) and scenarios; the system's interface to its environment is described in terms of actions, percepts and external data; and functionalities are defined.
- Architectural design: where agent types are identified; the system's overall structure is captured in a system overview diagram; and scenarios are developed into interaction protocols.
- Detailed design: where the details of each agent's internals are developed and defined in terms of capabilities, data, events and plans; process diagrams are used as a stepping stone between interaction protocols and plans.

Each of these phases includes models that focus on the dynamics of the system, (graphical) models that focus on the structure of the system or its components, and textual descriptor forms that provide the details for individual entities.

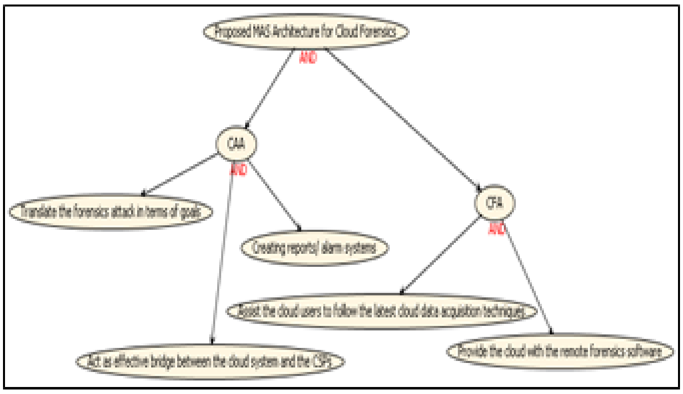
Proposed MAS Architecture for Cloud Forensics
AND
CAA
AND
CFA
AND
Translate the forensics attack in terms of goals
Creating reports/ alarm systems
Assist the cloud users to follow the latest cloud data acquisition techniques
Act as effective bridge between the cloud system and the CSPs
Provide the cloud with the remote forensics software

Fig. 4. MAS architecture Design Goals

4 Study

We have developed one hypothetical case study to achieve the main objective of our proposed approach that will help the CSP to automatically address the issue of the cloud forensic. The case study requires a reinterpretation when set in a cloud computing environment for the following problems:

- Acquisition of forensic data is more difficult.
- Cooperation from CSPs is paramount.
- Current forensic tools appear unsuited to process cloud data.
- Cloud data may lack key forensic metadata.
- Chain of custody is more complex.

Evidence collection from cloud computing is very crucial. Extracting data, preserving them, building hypothesis and presenting digital evidences can all aid in solving legal cases. In this paper, a real legal case is considered.

Cloud user (Arwa) renting an operation system for her mobile phone from a CSP as a SaaS (Software as a Service) after a SLAs has been issued them.

Case study incident summary: a cloud server (CSP) received a complaint from a cloud user (Arwa) explaining that the operating system of her mobile phone had been hacked. Her contact list has been receiving text messages (bad messages) through a popular chatting application. However, Arwa claims that she has not been sending any messages from her mobile. After accepting the case, the investigators started looking at the logs and records of this incident, and began a trace from Arwa's CSP.

In the technical report provided by the ISP, there are two registers of messages for servers of mobile phones: the cloud sender register and the cloud receiver register. The report indicates that the messages were actually received by Arwa's contact list. However, there was no record of her mobile having sent any messages.

Based on CSP's report, Arwa is innocent in this case. However, there is a need to know how was Arwa's phone compromised and used to send messages to Arwa's contacts. Arwa's phone was not available for testing due to legal constraints. There was a need to simulate the events to better understand the ways by which Arwa's phone was compromised.

To carry out cloud forensics and to better understand how such a compromise can take place, our proposed MAS architecture is used to examine and extract the data. Agents are used Agent Communication Language (ACL) for communication.

5 Testing

1. Cloud Acquiring Agent (CAA): this agent has two tasks as follow:
   - Dedicated for the collection step. Its role is the collection and the processing of the log files content.
   - Dedicated for the inspection step. It identifies suspected events in the collected log files content. This agent must transmit any suspected event to the investigation.
2. Cloud Forensics Agent (FCA): this agent has one task as follow:
   - Dedicated for the two main steps: investigation and notification. This agent has to check the suspected event and determine its significance and objective in order to confirm or refute the occurrence of attack. If any attack is confirmed, the FCA agent generates a detailed report and sends it to the security CSP as a security alert.

6 Finding

The CSP confirmed earlier that (Arwa) did not send messages. On the other hand, Arwa's contacts received messages from Arwa's phone. To simulate the scenario, a similar device was tested using our framework. It was found that messages do not necessarily require cellular communications to be delivered. Messages can also be delivered over Wi-Fi network. From the abovementioned facts we can derive two possible compromise scenarios. Scenario A, the Subscriber Identity Module (SIM) card was removed and the attacker used Wi-Fi network to deliver message. Scenario B, Arwa sold her phone but didn't delete application and the new owner used a Wi-Fi network to deliver messages to Arwa's contacts.

7 Results and Discussion

To evaluate the performance of our system against the scale of the system, we measure the times required for an agent to travel around different number of cloud users before and after the implementation. The results are presented in Table 1 and are plotted Fig. 5. The data show that the Round Trip Time (RTT) for an agent to travel in our system changes more or less linearly over the number of CSPs in the system, both the cases. This is due to the additional time to travel an additional CSP. The overhead for each additional CSP is more or less the same. The overhead introduced is due to the extensive use of the MAS architecture to forensics tools, techniques, attributes and law enforcement is high after the implementation of our proposed framework. Hence, a trade-off between performance and our proposed MAS architecture is identified.

Number of CSPs	RTT Before the implementation	RTT After the implementation
1	2043.7	3988.74
2	3013.46	6098.19
3	5945.7	7908.77
4	6880.197	9921.02
5	9040.71	11900.18
6	10713.9	14066.79
7	13605.4	16080.5
8	15076.7	17913.16
9	18002.43	19893.63
10	19901.623	22000

Table 1. Average of RTT of our MAS in cloud forensics

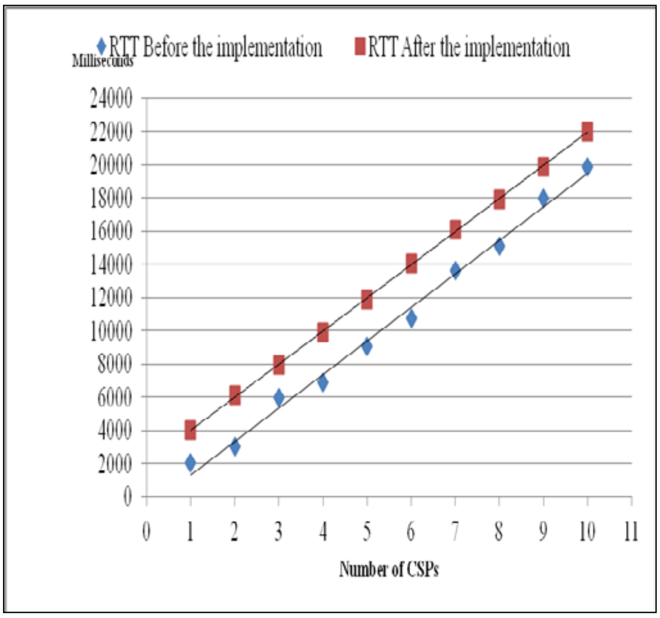

Fig. 5. Average of Round Trip Time (RTT) before and after the implementation

8 Conclusions

In this paper, we investigated the problem of digital forensics in cloud computing environment (cloud forensics), to ensure the cloud data acquisition, applying forensics law enforcement, provide the CSPs with the latest cloud forensics techniques, tools and attributes and to provide the cloud with the existing remote forensics software; we proposed cloud forensics framework and MAS architecture. This framework consists of two main layers as agent layer and cloud forensics layer that consist of CSP, law enforcement, forensics investigators and cloud user. The propose MAS architecture includes two types of agents: Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA). To formulate the cloud forensics framework for collaborative cloud computing environment, the components on MAS, CSP, forensics techniques, tools and attributes and forensics law enforcement are compiled from various literatures. The relationships between these components are used to construct the framework analysis. The result shows that performance of our proposed framed work based on Round Trip Time (RTT) for an agent to acquire the cloud forensics and measured by the times required for an agent to travel around different number of CSPs before and after the implementation is high after the implementation.

As a future research direction, cloud forensics as an open research area has to be further explored with newly adaptive frameworks that consider cloud user privacy, cloud data integrity, cloud data confidentiality, cloud data segregation, and many other factors. However, these frameworks should be incorporated with newly developed dynamic cloud forensic tools to cope with the cloud infrastructure.

References

[1] S. Biggs and S. Vidalis, "Cloud Computing: The Impact on Digital Forensic Investigations," In Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for, 2009, pp. 1-6.

[2] A. M. Talib, R. Atan, R. Abdullah, and M. Azrifah, "CloudZone: Towards an Integrity Layer of Cloud Data Storage Based on Multi Agent System Architecture," In Open Systems (ICOS), 2011 IEEE Conference on, 2011, pp. 127-132.

[3] M. Pollitt and A. Whitledge, "Exploring Big Haystacks," In Advances in digital forensics II: Springer, 2006, pp. 67-76.

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

[6] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," NIST Special Publication, pp. 800-86, 2006.

[7] S. Fugkeaw, P. Manpanpanich, and S. Juntapremjitt, "Multi-Application Authentication Based on Multi-Agent System," In IMECS, 2007, pp. 1316-1321.

[8] E. H. Durfee, V. R. Lesser, and D. D. Corkill, "Trends in Cooperative Distributed Problem Solving," Knowledge and Data Engineering, IEEE Transactions on, vol. 1, pp. 63-83, 1989.

[9] A. M. Talib, R. Atan, R. Abdullah, and M. A. A. Murad, "Towards a Comprehensive Security Framework of Cloud Data Storage Based on Multi Agent System Architecture," Journal of Information Security, vol. 3, p. 295, 2012.

[10] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet: Academic press, 2011.

[11] S. Thorpe, "An Experimental Survey Towards Engaging Trustable Hypervisor Log Evidence within A Cloud Forensic Environment," International Journal of Computer Science & Information Technology, vol. 4, 2012.

[12] F. Zambonelli, N. R. Jennings, and M. Wooldridge, "Developing Multi-agent Systems: The Gaia methodology," ACM Transactions on Software Engineering and Methodology (TOSEM), vol. 12, pp. 317-370, 2003.

[13] M. J. North, N. T. Collier, and J. R. Vos, "Experiences Creating Three Implementations of the Repast Agent Modeling Toolkit," ACM Transactions on Modeling and Computer Simulation (TOMACS), vol. 16, pp. 1-25, 2006.

[14] J. P. Bigus, D. A. Schlosnagle, J. R. Pilgrim, W. N. Mills Iii, and Y. Diao, "ABLE: A Toolkit for Building Multi-agent Autonomic Systems," IBM Systems Journal, vol. 41, pp. 350-371, 2002.

[15] V. S. Chawathe and B. B. Meshram, "Cloud Forensics-An IS Approach," 2012.

[16] D. Birk, "Technical Challenges of Forensic Investigations in Cloud Computing Environments," In Workshop on Cryptography and Security in Clouds, 2011, pp. 1-6.

[17] S. Zawoad and R. Hasan, "Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems," arXiv preprint arXiv:1302.6312, 2013.

[18] J. Dykstra and A. T. Sherman, "Acquiring Forensic Evidence From Infrastructure-as-a-service Cloud Computing: Exploring and Evaluating Tools, Trust, and Techniques," Digital Investigation, vol. 9, pp. S90-S98, 2012.

[19] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic Investigation of Cloud Computing Systems," Network Security, vol. 2011, pp. 4-10, 2011.

[20] National Institute of Standards and Technology. Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14. Available at http://www.ncjrs.gov/pdffiles1/nij/222982.pdf; 2008. Last accessed September 21, 2011.

[21] L. Padgham and M. Winikoff, Developing Intelligent Agent Systems: A practical guide vol. 13: John Wiley & Sons, 2005.