An Integrated Framework of Multi Software Agent and Cloud Forensics

ARWA IBRAHIM AHMED
Information Systems Department
Princess Nourah Bint Abdulrahman University (PNU), Riyadh
KINGDOM OF SAUDI ARABIA
Email: Ariahmed@pnu.edu.sa

Abstract: - Cloud computing is one of the most prominent technological trends as it provides a number of digital storage and services. However, evidence acquisition and investigation of violations occurring in cloud environment is still a critical issue in cloud forensics. This paper develops an integrated framework that consists two main layers are Cloud Forensics Layer (Cloud Service Provider, law enforcement, forensics investigators and cloud users), and Multi Agent System (MAS) architecture layer that includes two agents: Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA). The model is then tested based on the Cloud Forensic Capability Matrix (CFCM) using a sample covered the cloud actors who are cloud forensic practitioners and experts from cloud users, CSPs, academia, cloud broker, cloud investigators, and law enforcement. The proposed framework was supported, providing preliminary evidence that the two layers can and should be integrated. The integrated framework helps build a conceptual bridge to the cloud forensics.

Key-Words: - Cloud Computing Forensics, Multi Agent System, Cloud Forensic Capability Matrix, Digital Forensics, Integrated Framework, and Cloud Forensic Investigative Architecture.

1 Introduction

Cloud computing has become one of the most dominant topics in the computing industry, following the developments of mainframes, minicomputers, personal computers, and smart phones [1, 2]. It dramatically transforms the way information technology services are created, delivered, and managed by the enterprises [3]. According to Gartner [4], by 2015 up to 20% of non-IT Global 500 enterprises will be cloud service providers. However, the question that comes to mind is that the rapid growth of cloud computing adoption as a non-standard technology brings a digital forensics deeper into the crisis that it is facing? [3, 4].

Encryption, availability and uptime, number of concurrent users, proliferation of endpoints, application response time, the schedule for notification in advance of network changes that may affect users, multi-jurisdiction, specific performance benchmarks to which actual performance will be periodically compared, loss of data control, usage statistics that will be provided, and help desk response time for various classes of problems are among the challenges facing cloud computing for forensic investigations due to the lack of tools and expertise [5, 6].

A cloud forensic capability must be established to address these issues through signing a service-level agreements (SLAs) between Cloud Service Providers (CSPs) and cloud users, otherwise, they will face many challenges in investigation of critical incidents occurring in cloud environment such as violations, hacking, and major measures intrusions to restore data and services. They will also face difficulties to provide evidences for use in judicial proceedings in cases of resource confiscation, given the lack of forensic preparation [3].

Cloud Computing researchers have developed rich streams of research that investigate the critical criteria for cloud forensic. Commonly, researchers tie these criteria to user perceptions about cloud and how it impacts their usage, the opportunities and challenges facing cloud forensics, and the research direction for cloud forensics [3]. Despite researchers have addressed such perceptions in different ways, in general, there have been two dominant approaches employed which are cloud forensics [e.g. 3, 5, 7, 8], and agents based cloud computing [e.g. 9, 10-12]. Both research streams provide valuable contributions to our understanding of cloud forensics, although each tells only part of the story. The main aim of study is to integrate the two research streams so as in order to provide a more comprehensive understanding of cloud forensics.

Although cloud forensics and agents based cloud computing have evolved largely as parallel research

streams, the two approaches can and should be integrated [5, 9]. Such integration can assist in build a conceptual bridge to the cloud forensics. Ultimately, this would enhance the predictive value of cloud computing for forensic investigations, more response from CSPs, and improve the satisfaction of cloud users. Moreover, this integration can response to the call to provide a way for perception-based cloud computing research to more fully examine the role of the cloud forensics [5, 8].

To accomplish this, the paper develops a framework for cloud computing forensics that consists two main layers are Cloud Forensics Layer (Cloud Service Provider, law enforcement, forensics investigators and cloud users), and Multi Agent System (MAS) architecture layer that includes two agents: Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA). The contribution of this paper is identify the technical scenario of a crossing discipline of cloud computing forensics, and propose a digital cloud framework based on MAS architecture that helps applying cloud forensics.

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 method used in this study. Section V presents analysis and result. Section VI concludes the work.

2 Related Works

The digital forensics can be perceived as one of computer applications which concerns with collecting preserving, examining, analyzing, retrieving and presenting relevant digital evidence for use in judicial and criminal proceedings by law enforcement authorities [13, 14]. The most important issue in digital forensics is a judicial proceedings, thus, it must have a correct and sound procedure in carrying out the forensic investigation and conducting the inspection setup so that ensuring these procedures follow a systematic and scientific method to obtain a reliable evidences [15]. Recently, the use of digital forensics is no longer limited to a laboratory in police departments and security agencies, rather it widely utilized in several disciplines including cloud computing.

Cloud forensics is a subset of network forensics that work on the discipline of cloud computing and digital forensics [6]. Network forensics deals with forensic investigations of networks, while cloud computing is based on broad network access. Although the purpose of digital forensics and cloud forensics as a principle is the same in terms of evidence acquisition about the transactions, the procedures of forensic investigation and inspection setup in cloud computing requires fundamentally different tools and techniques than those in the traditional digital forensics [16, 17]. Cloud computing is a shared collection of configurable network resources such as networks, servers, storage, applications and services that can be reconfigured quickly with minimal effort [1]. Therefore, cloud forensics follows procedures of network forensics with techniques tailored to cloud computing environment [18].

Zawoad and Hasan [19] emphasized that the procedures of cloud forensics are vary drawing on the service and deployment model of cloud computing. They argue for Software as a Service (SaaS), and Platform as a Service (PaaS) there are very limited control over process or network monitoring. Whereas, it can gain more control in Infrastructure as a Service (IaaS) and can deploy some forensic friendly logging mechanism. The steps of computer forensics will vary for different services and deployment models. For instance, the processes of digital evidence acquisition for SaaS and IaaS will not be same. In the SaaS scenario, they solely depend on the CSPs 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.

A variety of researchers have developed schemas of cloud computing forensics. For example, Birk [18] suggest that the digital forensics evidence can be available in three different stages in cloud computing namely: Data at rest, data in motion, and in execution. Data at rest represents allocated disk space, the data in motion refers to the data transformation from one entity to another, while the execution reflects the data processing, machine instruction, and information about the current system state. In addition, Dykstra and Sherman [9] proposed a framework to assess the potential forensic acquisition techniques in cloud computing environment. This framework includes six layers are: guest application/data, guest OS, virtualization, host OS, physical hardware, and network. Moreover, the National Institute of Standards and Technology (NIST) has published a Digital Data Acquisition Tool Specification, which “defines requirements for digital media acquisition tools in computer forensic investigations” [20]. However, the last version of the specification was issued in 2004, i.e. before the emergence of cloud computing.

Although the availability of variety of studies that investigated the cloud computing forensics [3, 5, 6, 9, 16, 18, 19], these attempts are remain insufficient to provide a more complete understanding and knowledge about the cloud forensics. Many scholars indicated that evidence acquisition is still a critical issue in cloud forensics [9, 21, 22]. Ruan, et al. [6] stressed that the 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. Likewise, Taylor, et al. [22] 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]".

Some studies suggest that cloud computing forensics not easy task, rather it requires adoption of Intelligent Systems Agent-based Software [9, 19, 23]. This is due to the fact that the cloud generates a massive volume of data content within the data store of the CSPs. Thus, forensic inspection of all functional systems that dominate data processing, data sources and a proper understanding of files access and deletion can be a significant challenge via the traditional digital forensics [24]. Multi Agent System (MAS) enables an effective and accurate cloud forensics [23]. It also provides better understanding of cloud domain in specific way [10].

The Multi Agent System is perceived as a artificial intelligence technique which focuses on the system, so several agents communicate with each other through the Agent Communication Agent (ACL) [25]. It can be 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" [26]. Agents must be able to interact with each other to achieve a common goals. This interaction may lead to expose different types of behaviors such as selfish or benevolent behavior [25]. In the context of cloud forensics, the selfish agents ask for assistance 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 [24]. While, the benevolent agents often provide assistance to other agents because they consider system benefit is the top priority such as the agent that serving forensics law enforcement for CSPs service are always ready to assist other agents to complete their tasks [24].

Several research have developed multiple toolkits for agent-based software in different areas of IT [27-29]. They further mentioned that such agent-based software has a potential for digital forensics investigations. Yet, there is a lack of studies that address intelligent agent systems for cloud forensics investigations.

Therefore, this paper will fill the gap in literature by developing a framework for cloud computing forensics that involves cloud forensics architecture and MAS.

3 An Integrated Framework of Cloud Forensics and MAS

To capture a holistic insight of cloud forensics, we propose an integrated framework of cloud forensics and MAS. This framework has been built using two layers namely MAS layer and cloud forensics layer as shown in Figure 1.

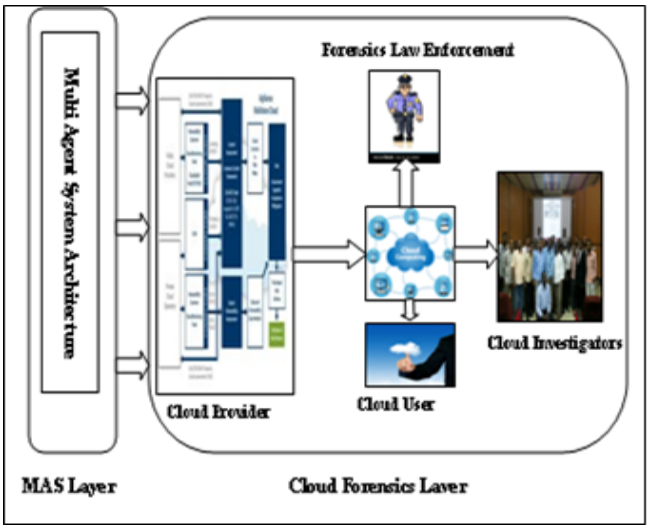

Fig.1. An integrated framework of cloud forensics and MAS

It is widely recognized that cloud forensic deals with investigations of different network entities [3]. Therefore, we begin to construct our framework with the right half of Figure 1. This framework serve as a shared system can be used by both CSPs and cloud users for cloud forensics investigations. The functionality of framework's layers can be summarized as follows:

3.1 Cloud Forensics Layer

Cloud data storage has four different network entities can be identified as follows [24]:

- Cloud Service Providers (CSPs): the entities who have a considerable resources and expertise distributed in building and managing cloud storage servers, as well as they own and operate cloud computing systems.
- Cloud Forensics Law Enforcement: represents the use or application of scientific knowledge

to a point of law, particularly in investigation of crime in cloud computing.

- Cloud Forensics Investigator: the individuals form both public and private sectors who are carrying out cloud forensics investigations such as researchers, lawyers, cloud experts, cloud companies, and others.
- Cloud User: the individual consumers and organizations who have data need to store in the cloud computing and they rely on the cloud for data computation.

To enable an effective cloud forensics investigation, this study proposed that this layer be integrated with Multi Agent System (MAS) layer.

3.2 Multi Agent System (MAS) Layer

This layer has two agents: the Cloud Acquiring Agent (CAA), and Cloud Forensics Agent (FCA). The scenarios of the agents are summarized as follow:

3.2.1 Cloud Acquiring Agent (CAA)

In CAA scenario as depicted by Figure 2, the simplest scenario for CAA interaction is provided. In service provision, 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 a Service Level Agreement (SLA1) with the provider. In contrast, the CSP signs another separate 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 share the 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.

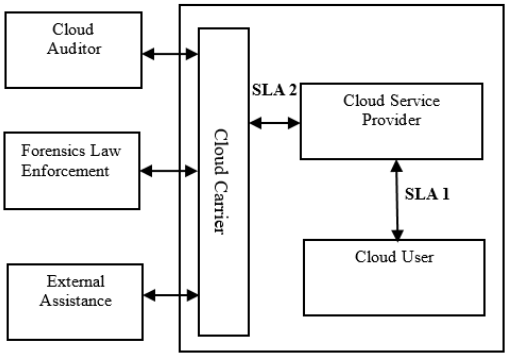

Fig 2. Cloud Acquiring Agent (CAA) Scenario

3.2.2 Cloud Forensics Agent (FCA)

In Cloud Forensics Agent (FCA) scenario as depicted by Figure 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 set 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.

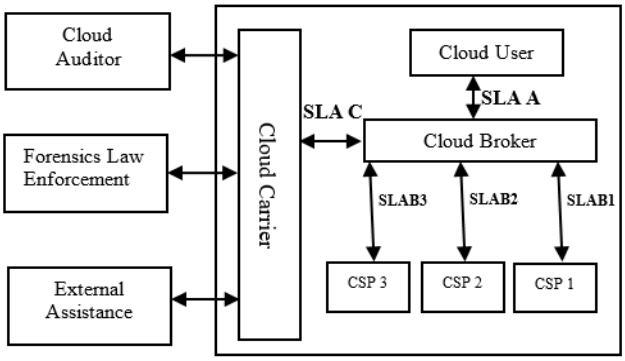

Fig 3. Cloud Forensics Agent (CFA) Scenario

4 Method

To ensure that the proposed framework meets its objective in cloud forensics, the MAS architecture is designed to determine the types of agents, events, protocols and agent capabilities drawing on the Prometheus methodology [30]. The Prometheus methodology includes three main phases are:

- System Specification: where the system is specified using goals (as illustrated in Figure 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 involves models that concentrate 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.

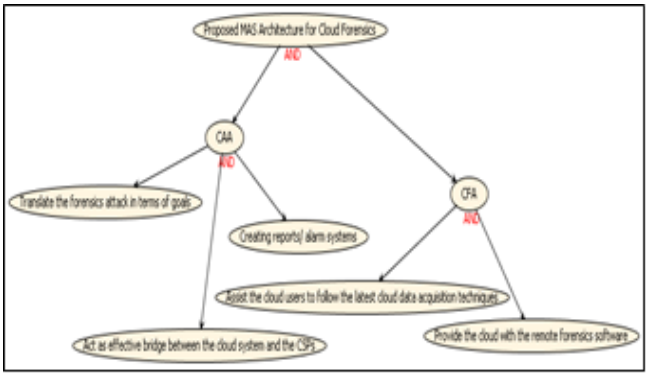

Fig. 4. MAS architecture Design Goals

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 [9, 22]. 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. The scenario of case study incident is summarized as follows:

- The Information Systems Department at Princess Nourah Bint Abdulrahman University (ISDPNU) rented an operation system as a SaaS from the CSP for 10 mobile phone's users "Cloud Users", and the SLA between ISDPNU and CSP has been signed.
- A cloud server (CSP) received a complaints from some cloud users that the operating system of their mobile phones has been hacked by receiving bad text messages through a popular chatting application. The users claimed that they have not been sending any messages from their mobile phones. After accepting the case, the investigators started looking at the logs and records of this incident, and began a trace from users' 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 users' contact list. However, there was no record of their mobile phones having sent any messages.
- Based on CSP's report, the users are innocent in this case. Nevertheless, there is a need to know how was users' phones compromised and used to send messages to the users' contacts. The users' phones were not available for testing due to legal constraints. There was a need to simulate the events to better understand the ways by which users' phones were compromised.

As part of the validation process, the suggested framework has been evaluated based on the Cloud Forensic Capability Matrix (CFCM) developed by Ruan and Carthy [31]. The CFCM has developed drawing on the Cloud Forensic Investigative Architecture (CFIA), and the Capability Maturity Model (CMM) for Software proposed by Paulk [32]. The CFCM is a capability maturity model to evaluate and improve cloud forensic for any given cloud actor including cloud users, CSPs, cloud carrier, cloud broker, cloud investigators, and cloud law enforcement. The CFCM model includes four key categories of cloud forensic capabilities corresponding to the CFIA as listed in table 1. The model suggests that these capabilities are the main basis for CFCM.

Table 1. Cloud Forensic Capabilities

Cloud Forensic Capabilities	**Description**
Pre-investigative capabilities	Capabilities in preparation for investigation process whether internal or external.
Investigative capabilities	Capabilities needed to the core investigative process.
Supportive capabilities	Capabilities needed to support and complete the investigation case.
Interfacing capabilities	Capabilities concerned with the internal and external interface between the cloud computing environment and investigative entities that involved in cloud forensic investigations.

Each capability embraces a group of criteria in technical, legal and organizational dimensions as shown in Figure 5. According to Ruan and Carthy [31], these criteria serve as a measurements to assess any enhancements and developments of cloud forensics.

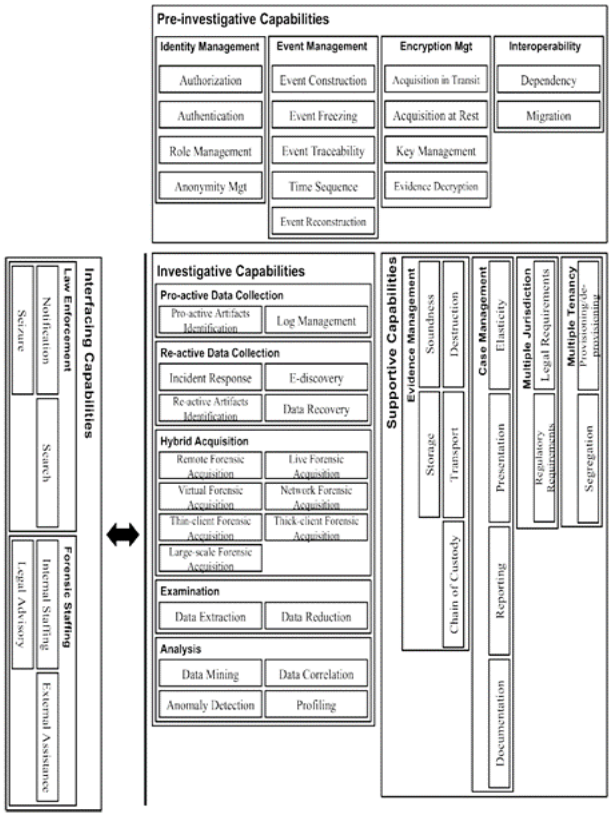

Fig. 5. The Cloud Forensic Capability Matrix (CFCM).

A survey was undertaken to verify the proposed framework. The survey covered the cloud actors who are cloud forensic practitioners and experts from cloud users, CSPs, academia, cloud broker, cloud investigators, and law enforcement. Table 2 shows the respondents of this study. They invited to attend the hypothetical case study, and then asked to evaluate the proposed framework after explaining the functionality of the proposed framework.

Table 2. Respondents

Cloud Actors		**Number**
1	Cloud Users	10
2	CSPs	2
3	Academics	6
4	Cloud Broker	2
5	Cloud Investigators	3
6	Law Enforcement	2
	Total	25

5 Analysis and Result

To carry out cloud forensics and to better understand how such a compromise can take place, our proposed framework is applied using MAS architecture to examine and extract the data for forensics. Agents are used Agent Communication Language (ACL) for communication. The tasks of CAA and FCA has been identified as follow:

1. Cloud Acquiring Agent (CAA) has two tasks are:
   - Dedicated for the collection step (collection and 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 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.

The hypothetical case study discussed earlier confirmed that the CSP acknowledged that the cloud users did not send messages. In the contrast, they received a bad messages on their phones. To simulate this scenario using our proposed framework, a similar devices were tested. The findings indicate that the messages do not necessarily require cellular communications to be delivered. It can also be delivered over Wi-Fi network. From the abovementioned facts we can extract two possible compromise scenarios. The first scenario is the Subscriber Identity Module (SIM) card, which assumes that the SIM was removed and the attacker used Wi-Fi network to deliver message. While the second scenario is that the users sold their phones but didn't delete application and the new owners used a Wi-Fi network to deliver messages to the contacts.

To evaluate our proposed framework against the criteria of cloud forensic capabilities, a panel of 25 cloud forensic experts and practitioners was invited to assess the suggested framework based on their observations and perceptions about the hypothetical case study, and then the panel members were asked to evaluate the capabilities of MAS-based cloud forensic framework based on the CFCM criteria.

The findings of this study showed that the vast majority of respondents firmly agree that the proposed framework of MAS-based cloud forensic improves the cloud forensic capabilities including pre-investigative, investigative, supportive and interfacing capabilities. Table 3 illustrates the results of evaluation.

Table 3. Evaluation the Capabilities of MAS-based Cloud Forensic

Criteria of Cloud Forensic Capabilities		% Agree
Pre-investigative capabilities		
Identity management	The MAS-based cloud forensic able to manage user's identities, their authorization, authentication, roles and permissions to access system resources in the cloud environment.	98%
Event management	The MAS-based cloud forensic has a potential to conceptually construct the unit of an "event" and technically execute that concept so that it can be constructed, reconstructed, traced when needed, and frozen as a crime scene under investigation when required.	97%
Encryption management	The MAS-based cloud forensic has the ability to search, access and acquire encrypted data for forensic investigations in shared cloud environment without violating privacy or incompliance with data protection regulation within a particular jurisdictions.	95%
Interoperability	The MAS-based cloud forensic ensures forensic readiness in inter-cloud environments (dependency and migration).	97%
Investigative Capabilities		
Pro-active data collection	The MAS-based cloud forensic has a potential to maximize the use of digital evidence while cutting down the cost of an investigation.	99%
Re-active data collection	The MAS-based cloud forensic able to trigger forensic data collection after an incident immediately, and it also able to reveal and retrieve the data after a period of time when the incident discover internally within the system or externally notified by the law enforcement.	97%
Hybrid acquisition	The MAS-based cloud forensic enhances the ability to search, access, and acquire forensic data from many different layers and components within cloud environment.	98%
Examination	The MAS-based cloud forensic enables to investigate forensic data collected from the collection phase to develop input for further forensic investigation and analysis.	95%
Analysis	The MAS-based cloud forensic improves the forensic data analysis and contributes to create analysis result as digital evidence.	95%
Supportive Capabilities		
Evidence management	The MAS-based cloud forensic guarantees the digital forensic evidences are kept and handled in a manner that ensures the integrity of evidence during the evidence timeline (from acquisition, investigations, verification, analysis, transform, storage, presentation, to disposal) in order to provide an acceptable and reliable evidence to law enforcement authorities.	92%
Case management	The MAS-based cloud forensic ensures an effective management for the case under investigation in a sufficient, appropriate, and well-archived manner.	91%
Multi-jurisdiction	The MAS-based cloud forensic provides a better and clearer understanding for legislative and regulatory requirements and clarifies forensic process under multiple jurisdictions.	97%
Multi-tenancy	The MAS-based cloud forensic enhances the ability of all cloud entities to provide and extract forensic evidence among multiple tenants who are sharing same computing resources. In addition it enables to separate tenants' data during the investigation process.	95%
Interfacing Capabilities		
Law enforcement	The MAS-based cloud forensic achieves a better interfacing of law enforcement among cloud entities in cases of external investigations while reducing internal loss.	96%
Forensic staffing	The MAS-based cloud forensic improves the ability of a cloud entities to organize a functional staffing structure in order to facilitate the investigation process whether internal or external.	94%

5 Conclusion

This paper integrated the cloud forensics and MAS architecture 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. It developed a framework of cloud forensics and MAS architecture. This framework consists two main layers are cloud forensics layer that includes the CSP, law enforcement, forensics investigators and cloud user. While, the MAS architecture layer

contains two types of agents: Cloud Acquiring Agent (CAA) and Cloud Forensics Agent (FCA). The proposed framework has been tested using Cloud Forensic Capability Matrix (CFCM). The results shown that the proposed framework improves the cloud forensic capabilities including pre-investigative, investigative, supportive and interfacing capabilities.

This study has some limitations although it is among an initial steps to enhance the knowledge about cloud forensics. It was limited to small sample, therefore, to enhance the validity of the proposed framework, this study suggests conducting further research using wider sample. In addition, it will be useful to apply the proposed framework in other cloud scenarios such as Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In fact, the cloud forensics is still new and open research area that requires further investigation. The suggested framework can be further extended by incorporating it with new developed dynamic cloud forensic tools that consider cloud user privacy and confidentiality issues, data integrity, and data segregation.

References:

[1] O.-S. Lupşe, M. M. Vida, and L. Tivadar, "Cloud computing and interoperability in healthcare information systems," in *The First International Conference on Intelligent Systems and Applications*, 2012, pp. 81-85.

[2] H. Sulaiman and A. I. Magaireah, "Factors affecting the adoption of integrated cloudbased e-health record in healthcare organizations: a case study of Jordan," in *Information Technology and Multimedia (ICIMU), 2014 International Conference on*, 2014, pp. 102-107.

[3] K. Ruan, J. Carthy, and T. Kechadi, "Survey on cloud forensics and critical criteria for cloud forensic capability: A preliminary analysis," in *Proceedings of the Conference on Digital Forensics, Security and Law*, 2011, p. 55.

[4] P. Gartner, "Top Predictions for IT Organizations and Users for 2012 and Beyond," *Gartner, press release*, vol. 1, 2011.

[5] J. Dykstra and A. T. Sherman, "Understanding issues in cloud forensics: two hypothetical case studies," in *Proceedings of the Conference on Digital Forensics, Security and Law*, 2011, p. 45.

[6] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," *Digital Investigation*, vol. 10, pp. 34-43, 2013.

[7] T. V. Lillard, *Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data*: Syngress Publishing, 2010.

[8] S. Zargari and D. Benford, "Cloud forensics: Concepts, issues, and challenges," in *Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on*, 2012, pp. 236-243.

[9] 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.

[10] J. O. Gutierrez-Garcia and K. M. Sim, "Agent-based cloud service composition," *Applied intelligence*, vol. 38, pp. 436-464, 2013.

[11] K. M. Sim, "Agent-based cloud computing," *IEEE Transactions on Services Computing*, vol. 5, pp. 564-577, 2012.

[12] S. Venticinque, L. Tasquier, and B. Di Martino, "Agents based cloud computing interface for resource provisioning and management," in *Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on*, 2012, pp. 249-256.

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

[14] M. Pollitt and A. Whitledge, "Exploring big haystacks," in *IFIP International Conference on Digital Forensics*, 2006, pp. 67-76.

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

[16] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet*: Academic press, 2011.

[17] 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, p. 125, 2012.

[18] D. Birk, "Technical challenges of forensic investigations in cloud computing environments," in *workshop on cryptography and security in clouds*, 2011, pp. 1-6.

[19] S. Zawoad and R. Hasan, "Cloud forensics: a meta-study of challenges, approaches, and open problems," *arXiv preprint arXiv:1302.6312*, 2013.

[20] NIST, "Test Results for Digital Data Acquisition Tool: FTK Imager 2.5.3.14. ," National Institute of Standards and Technology2008.

[21] T. Kechadi, M. Faheem, and N. A. Le-Khac, "The State of the Art Forensic Techniques in Mobile Cloud Environment: A Survey, Challenges and Current Trends," *International Journal of Digital Crime and Forensics*, vol. 7, pp. 1-19, 2015.

[22] M. Taylor, J. Haggerty, D. Gresty, and D. Lamb, "Forensic investigation of cloud computing systems," *Network Security*, vol. 2011, pp. 4-10, 2011.

[23] V. S. Chawathe and B. B. Meshram, "Cloud Forensics-An IS Approach," *Journal of Computer Engineering*, vol. 4, pp. 45-48, 2012.

[24] 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.

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

[26] E. H. Durfee, V. R. Lesser, and D. D. Corkill, "Trends in cooperative distributed problem solving," *IEEE Transactions on knowledge and data Engineering*, vol. 1, pp. 63-83, 1989.

[27] J. P. Bigus, D. A. Schlosnagle, J. R. Pilgrim, W. N. Mills III, and Y. Diao, "ABLE: A toolkit for building multiagent autonomic systems," *IBM Systems Journal*, vol. 41, pp. 350-371, 2002.

[28] 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.

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

[30] L. Padgham and M. Winikoff, *Developing intelligent agent systems: A practical guide* vol. 13: John Wiley & Sons, 2005.

[31] K. Ruan and J. Carthy, "Cloud forensic maturity model," in *International Conference on Digital Forensics and Cyber Crime*, 2012, pp. 22-41.

[32] M. Paulk, "Capability maturity model for software," *Encyclopedia of Software Engineering*, 1993.