

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/276277635>

# Cloud Forensics Challenges

Conference Paper · February 2014

CITATIONS

0

READS

76

3 authors, including:



**Saad Alqahtany**

University of Plymouth

6 PUBLICATIONS 4 CITATIONS

[SEE PROFILE](#)



**Steven Furnell**

University of Plymouth

328 PUBLICATIONS 2,920 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



Federated Authentication Using the Cloud [View project](#)



A Forensically Enabled Cloud Computing Architecture in IaaS [View project](#)

All content following this page was uploaded by [Saad Alqahtany](#) on 14 May 2015.

The user has requested enhancement of the downloaded file. All in-text references [underlined in blue](#) are added to the original document and are linked to publications on ResearchGate, letting you access and read them immediately.

## Cloud Forensics Challenges

Saad ALQAHTANY, Nathan CLARKE & Steven FURNELL

Centre for Security, Communications and Network Research (CSCAN)

School of Computing and Mathematics, Plymouth University, PL48AA, Tel 01752586287

[saad.alqahtany@plymouth.ac.uk](mailto:saad.alqahtany@plymouth.ac.uk)

### **Abstract**

Cloud computing is a dramatic paradigm shift in the Information and Communication Technology era and it is transforming how services are being delivered. Cloud services are rapidly growing together with the acceptance rate and adoption of cloud solutions. The features of cloud computing such as resource pooling, rapid elasticity and large storage capacity along with its distributed nature present a range of technical and organisational issues for digital investigators. These issues lead digital investigators to have limited success when applying traditional forensic investigation approaches and tools. To date, there has been a significant lack of research focused upon solving cloud forensics issues. This paper discusses the definition of cloud computing, presents the forensic challenges pertaining to the cloud environment and proposes a framework using cloud features to overcome some technical cloud forensics issues with a view outlining the future prospects.

**Keywords-** *Cloud Computing, Digital Forensics, Cloud Forensics.*

### **1. Introduction:**

Cloud computing technologies have significantly changed the way in which organisations implement the building of their information technology infrastructure. Organisations outsource their IT infrastructure to third party providers. The cloud provider replaces it with virtualised, remote on-demand software services ([Grispos et al. 2011](#)). Organisations which moved their IT infrastructure from an outsourced data centre to a cloud provider could obtain a 37% cost saving and would eliminate 21% of the support calls for their system (Khajeh-

hosseini & Greenwood 2010). Whilst cloud computing clearly offers significant opportunities for organisations, issues surrounding the security and subsequent incident management requirements are frequently ignored leading to devastating consequences (Josshua 2012). Therefore, foundational development of a forensically-enabled cloud framework at the current stage of cloud development is a future essential aspect of a successful cloud environment. The structure of this paper is divided into seven sections: Introduction, cloud computing, cloud forensics, cloud forensics challenges, related work, proposed framework and conclusion.

## **2. Cloud Computing:**

Cloud computing will deliver computing resources as utilities in the same way that familiar utilities are delivered, (i.e. gas, water and electricity), the user will access services on demand and pay for the use. NIST 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” (Mell & Grance 2011). It is essential to identify cloud computing characteristics in order to understand their impact upon security and digital forensics. There are six essential characteristics, namely: on demand self-service, broad network access, resource pooling, location independence, rapid elasticity and pay-per-use business ([Almulla et al. 2013](#)). Furthermore, there are three main service models. The first is Infrastructure as a Service (IaaS), where a full computer infrastructure is delivered as a service via the Internet. The second is Platform as a Service (PaaS), where users can access and utilise a development platform online. The third is Software as a Service (SaaS), where turnkey applications are delivered via the Internet. Currently, there are four deployment models, namely: public, private, community and hybrid cloud. After reviewing the general concept of cloud

computing, the following section considers cloud forensics concepts followed by their challenges and opportunities for forensics investigators.

### 3. Cloud Forensics:

According to Zawoad & Hasan (2013), cloud forensics can be defined as the application of computer forensics principles and procedures in a cloud computing environment. Although cloud computing provides many promising economic and technological advantages such as more efficient use of resources, greater availability on a massive scale and reduced costs, there are serious concerns associated with it which must be addressed and overcome. According to a survey conducted by the International Data Corporation (IDC 2010), the issue of security is listed as the top concern of cloud adoption as shown in figure 1.

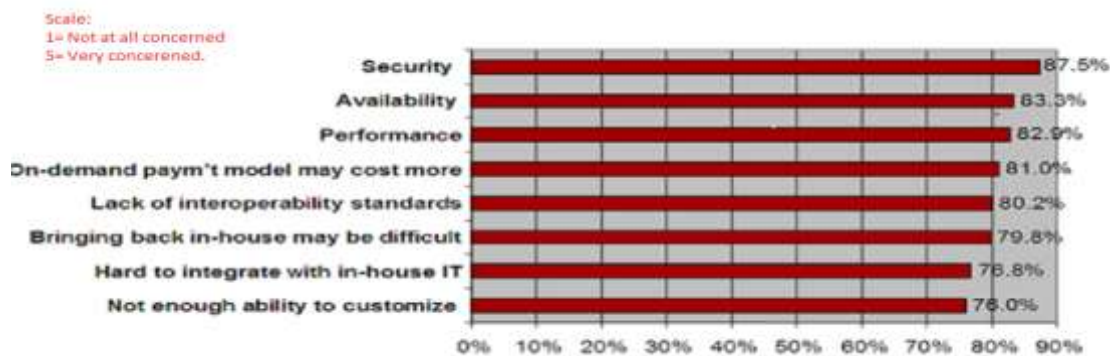


Figure 1 Rate the challenges of the cloud on demand model (IDC 2010)

Researchers believe that cloud computing is fraught with security challenges. Successful attacks on the cloud base can grant the attacker full power over the victims and all of the stored data. For example, in 2011, hackers successfully rented Amazon's servers and undertook the second largest online data breach in U.S history (Ruan & Carthy 2012). It is evident that it would have been impossible for the hackers to gain access to such critical information if the attack was not cloud-based. While researchers have found that security is still an "afterthought" during cloud adoption, Ruan & Carthy (2012) state that forensic implementation during cloud adoption has been an "after-after thought" compared to security.

#### **4. Cloud Forensics Challenges:**

This section identifies the most important issues pertaining to the cloud forensics.

##### **4.1. Physical accessibility:**

Cloud data is distributed among many hosts, this leads to a lack of knowledge about where data is exactly stored. Thus, it is difficult to place the events in a timeline or to analyse the sequence of events in a particular transaction ([Guo et al. 2012](#)).

##### **4.2. Dependence on the Cloud Services Providers:**

In the collection phase of digital forensics, we mostly rely on cloud service providers (CSP) who have the power over the cloud infrastructure and often do not let their customers see what is behind their virtual curtain (Birk 2011).

##### **4.3. Multi-tenancy:**

This means that multiple tenants share the same computing resources (Ruan and Carthy 2012). Thus, during the investigation process, we must maintain the privacy of other users and also ensure that suspect's data are not mixed with other users' data (Zawoad & Hasan 2013).

##### **4.4. Logs issues:**

Logs are very rich with invaluable analytical data, and digital investigators can pick useful evidence from them including application logs and networks logs. However, Zawoad & Hasan (2013) have identified the challenges that digital investigators face when analysing the logs:

**4.4.1 Decentralisation:** In the cloud infrastructure, there is no one single server to log users' data, so multiple users' data logs may be spread between many different servers.

**4.4.2 Volatility:** once the user turns off the power or exits the cloud, all logs data will be unavailable.

**4.4.3 Multi layers of logs:** there are many layers that investigators can collect log data from, such as the application, network and database; however, collecting and correlating data from different layers in a cloud infrastructure is not a simple process. Moreover, users often have to depend on the CSP to get log data especially in the SaaS model where the users have no ability to obtain logs.

#### **4.5. Multi- jurisdiction:**

The issues related to multi jurisdiction introduce many legal questions which have not been answered yet. According to Ruan et al (2011), there is a lack of legislative mechanisms that allow law enforcement agencies across the world to collaborate in cases such as cloud confiscation, evidence retrieval and data exchange.

### **5. Related work:**

Logging is regarded as the most part includes invaluable analytical data to the digital investigators. However, some researchers have proposed logs solution but with its limitations. For example, Trenwith and Venter (2013) have proposed a centralised logging of all activities for all participants to the cloud. Nevertheless, their model was developed to collect log evidence from Windows platforms only as well as other platforms and other types of evidence were not addressed by this model. Furthermore, the snapshots method is regarded as a powerful tool in a virtual environment, in which an investigator, through just one click, is able to clone a virtual machine including the running system memory (Birk 2011).

### **6. A Forensically-Enabled Cloud Computing Framework**

In order to deliver secure and smooth cloud services, it is vital to add an exclusive forensic-layer that will be incorporated within the cloud to enable cloud forensic investigation. This

will help the cloud provider to reduce the cost of conducting digital investigation and maximise its potential in order to extract digital evidence in a timely manner. However, current cloud infrastructures are fundamentally unable to achieve these requirements. Forensically-Enabled Cloud Computing Framework (FECF) is designed to capitalise cloud features including: centralised data, the massive storage, high availability and intensive computer resources. These features will quickly and effectively process and analysis intensive forensic jobs such as examining large volumes of data which can be extracted from different distributed systems. This framework as shown in Figure 2 illustrates a conceptual solution that can provide forensics evidences thereby capitalising cloud features.

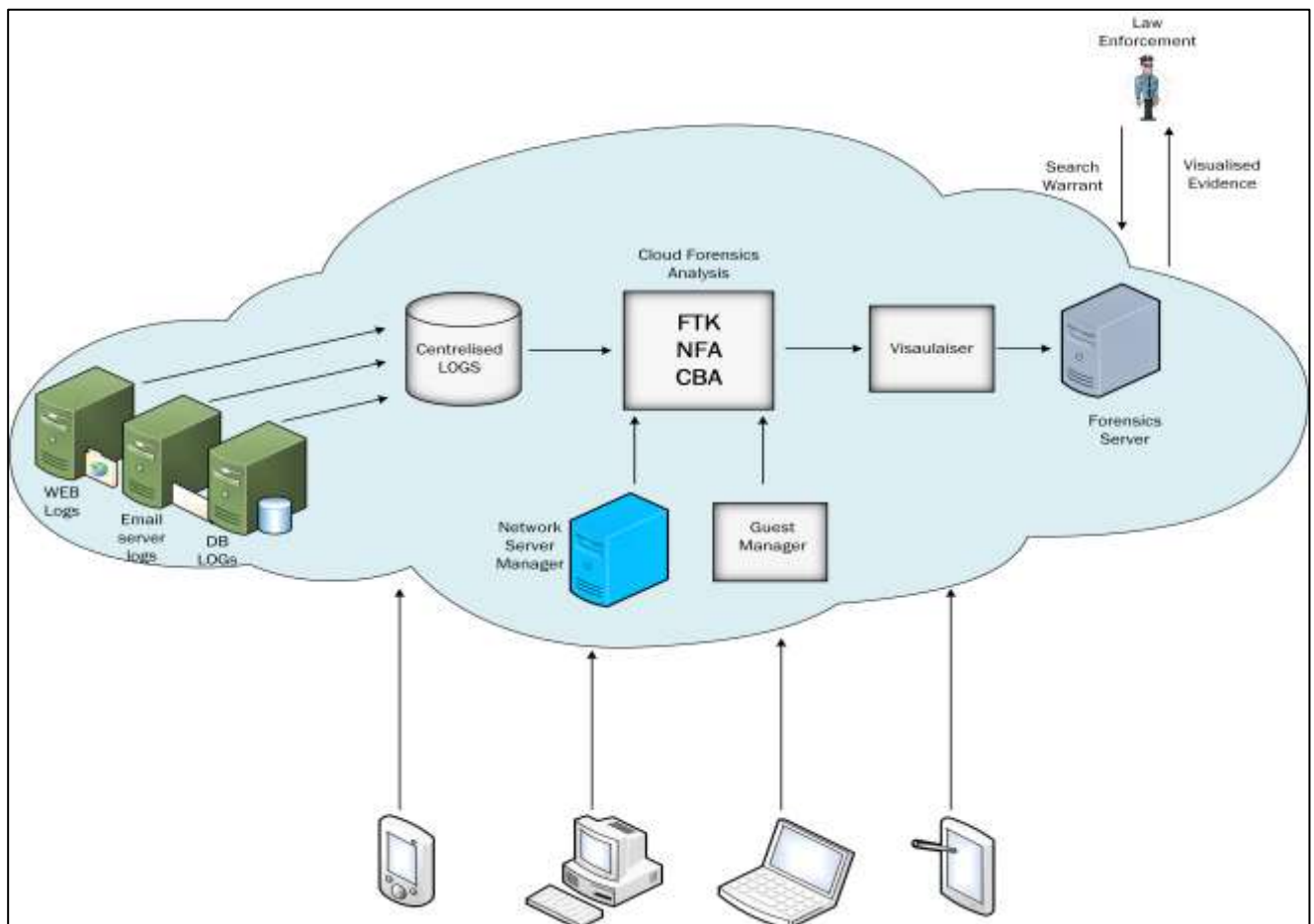


Figure 2 A Forensically-Enabled Cloud Computing Framework

This model works as follows: Centralised logs DB stores all activities for all participants to the cloud, Guest manager will extract guest application/data and network manager will

capture packets. All these potential sources of data will be sent to cloud forensics Analyser (CFA) which incorporates file system analysers (FTK or Encase), network forensic analysers (NFA) and cloud-based analysers (CBA). Evidence visualisation (visualiser) will help digital investigators to focus on specific crime-related evidences. Finally, visualised and analysed evidence will be stored at Forensics Server and be available when needed by law enforcement agencies.

## **7. Conclusion:**

Cloud computing has a range of unique features in order to deliver low cost services to multi-tenants. These features produce serious challenges to digital forensics investigators including unknown physical location, multi-jurisdiction and multi tenancy issues. However, cloud computing brings unique opportunities for a digital investigation process, such as centralised data, massive storage and the snapshot methods in a virtual environment. Current forensics approaches and tools cannot overcome all the aforementioned challenges. As such, extra research and developments are needed in different facets of the problem domain, including the technical, organisational and legal perspectives.

This paper has summarised cloud challenges in relation to cloud forensics and proposes a framework that would have the potential to overcome some of technical issues. Furthermore, having such solution can strengthen evidence admissibility in the court and will provide a better resources utilisation including time and finance. However, there are other key components have to be considered such as isolation and integrity of data being analysed.

## **References:**



Almulla, S., Iraqi, Y. and Jones, A. (2013). Cloud forensics: A research perspective. In *9th International Conference on Innovations in Information Technology (IIT)*. Abu Dhabi: Ieee, pp. 66–71. [online]. Available from: <http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6544395>.

Birk, D. (2011). Technical Challenges of Forensic Investigations in Cloud Computing Environments. , pp.1–6.

Grispos, G., Glisson, W. and Storer, T. (2011). Calm before the Storm: The Emerging Challenges of Cloud Computing in Digital Forensics. *dcs.gla.ac.uk*, pp.1–38. [online]. Available from: <http://www.dcs.gla.ac.uk/~tw/papers/grispos11calm-rev2425.pdf> [Accessed May 30, 2013].

Guo, H., Jin, B. and Shang, T. (2012). Forensic Investigations in Cloud Environments. In *2012 International Conference on Computer Science and Information Processing ( CSIP)*. Xi'an, Shaanxi: Ieee, pp. 248–251.

IDC. (2010). *IDC eXchange » Blog Archive » New IDC IT Cloud Services Survey: Top Benefits and Challenges*. [online]. Available from: <http://blogs.idc.com/ie/?p=730> [Accessed July 22, 2013].

Josshua, G. (2012). Protection in the cloud: Risk management and insurance for cloud computing. *Internet Law*, 15(12).

Mell, P. and Grance, T. (2011). *The NIST Definition of Cloud Computing, Recommendations of the National Institute of Standards and Technolog*. Gaithersburg, MD. [online]. Available from: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:The+NIST+Definition+of+Cloud+Computing+Recommendations+of+the+National+Institute+of+Standards+and+Technology#4> [Accessed July 12, 2013].

Ruan, K. et al. (2011). Cloud forensics : An overview. *IBM Ireland Ltd*, pp.1–16.

Ruan, K. and Carthy, J. (2012). Cloud Forensic Maturity Model. In *Digital Forensics and Cyber Crime*. Springer Berlin Heidelberg, pp. 22–41. [online]. Available from: [http://cloudforensicsresearch.org/publication/2012\\_Cloud Forensic Maturity Model\\_4thICF2C\\_Springer.pdf](http://cloudforensicsresearch.org/publication/2012_Cloud%20Forensic%20Maturity%20Model_4thICF2C_Springer.pdf) [Accessed November 21, 2013].

Trenwith, P.M. and Venter, H. (2013). Digital Forensic Readiness in the Cloud. In *Information Security for South Africa, 2013*. pp. 1–5.

Zawoad, S. and Hasan, R. (2013). Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. *Cryptography and Security*, pp.1–15.