Cloud Forensics: A Review of Challenges, Solutions and Open Problems

Saad Alqahtany ,Nathan Clarke & Steven Furnell

Centre for Security, Communications and Network Research, Plymouth University

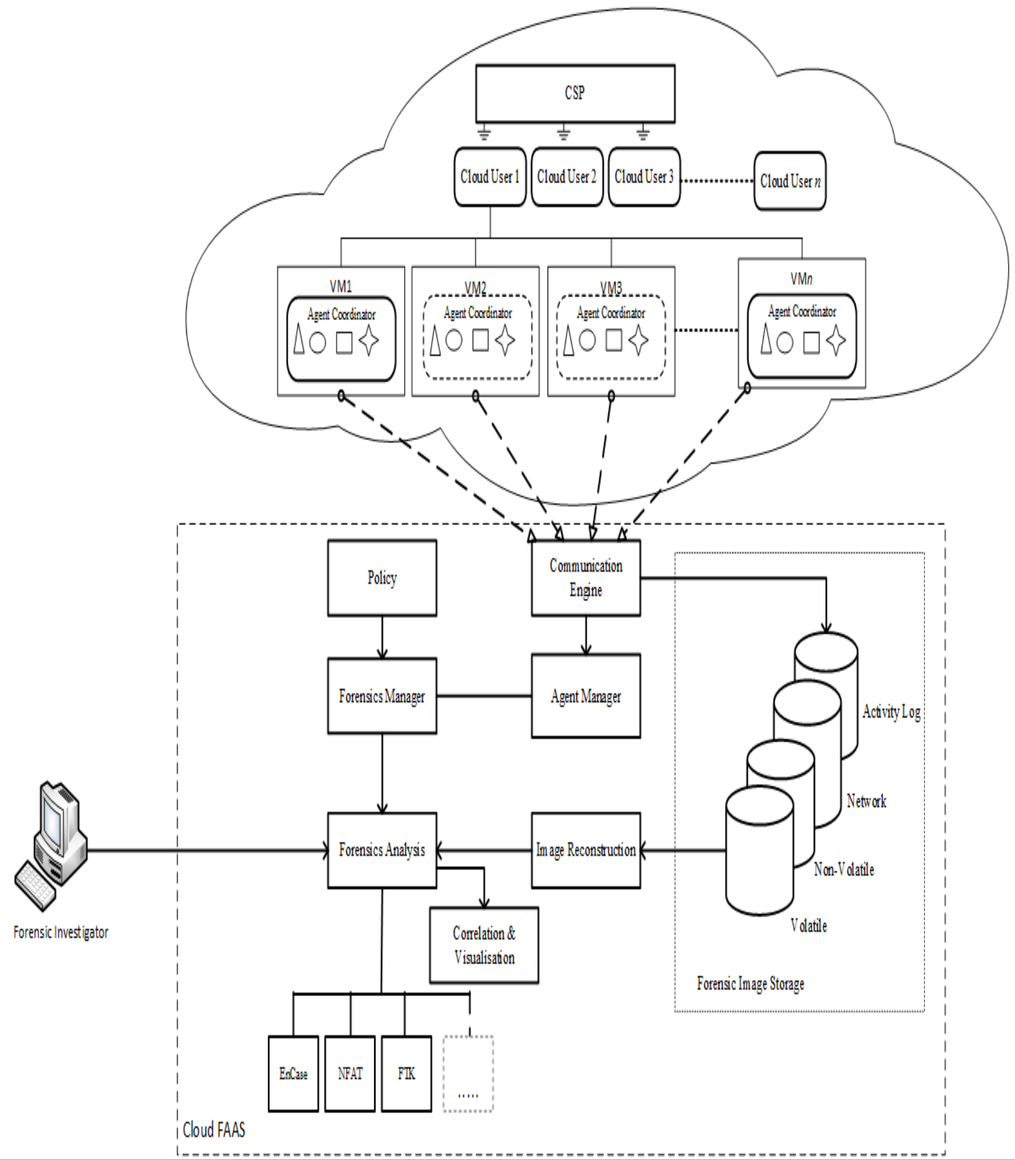
Saad.alqahtany@plymouth.ac.uk

Abstract

In the past few years, Cloud Computing has become attracted solution to many Internet and organisations and has become one of the hottest topics in IT. Despite the many benefits cloud computing introduces for the organisation, it will also present opportunities for criminal exploitation leaving almost no evidence behind. When the evidence resides in the cloud, new challenges exist on how to apply current digital forensic procedures. These challenges are novel and unique to the cloud and not encountered in traditional digital systems. Unfortunately, the distributed nature and configuration of cloud computing infrastructure introduces a range of problems for digital investigators. To date, the researchers have focused on identification of the foremost issues face digital forensic investigators when performing digital investigation in cloud computing. This poster extracts a view of recent interests based on investigating of relevant scientific documents on cloud forensic arena. It identifies the major challenges, summarises the available technical solutions and matches the identified solutions with the addressed challenges. Ultimately, the open problems in the area of cloud forensics are summarised based on a detailed literature with a view outlining the future prospects.

Open Issues	
1	Tackle the dependence on the cloud services providers
2	Timeline analysis across multiple sources and evidence correlation
3	Overcome the cross border issues
4	Lack control of the system
5	Jury's technical comprehension

Proposed Framework



Cloud Forensics challenges/ Process		Apply to Service model			Possible Solution	Ref
		IaaS	PaaS	SaaS		
Identification						
Access to the evidence		Partly	√	√	Eucalyptus framework	Zaferullah et al. (2013)
		X	√	√	a log-based model	Sang (2013)
Dependence on CSP for	Trust issue	√	√	√	Layers of Trust Model	Dykstar et al (2012)
		√	√	X	TrustCloud	Ko et al. (2011)
	Data acquisistion	√	√	√	Cloud Management Plane	Dykstra (2012)
	Compliance	√	√	√	SAL	Dykstra (2011), Biggs & Vidalis (2009)
	Logs	√	√	√	API provided by CSPs	Birk et al (2011)
Lack of customer awareness		√	√	√		Ruan et al. (2011)
Volitile data		√	X	X	Client Persistant Storage	Damshenas et al. (2012)
		√	√	X	A continuous synchronisation API	Birk et al. (2011)
Preservation & Collection						
Data integrity		√	√	√	Trust Platform Module (TPM)	Birk et al (2011), Dykstra (2012)
Time synchronisation		√	√	√	Unified/specfic time system	Damshenas et al. (2012)
Cloud literacy of investigators		√	√	√	Developing investigatores technical skils	Chen et al., (2012)
Analysis & Examination						
Lack of forensic tool		√	√	X	FROST, OWADE	Dykstra & Sherman (2013), (Kumar, 2011).
Presentation						
Jury's technical comprehension		X	X	X	--	Reilly et al (2011)