Analysis of Digital Investigation Techniques in Cloud Computing Paradigm

M.N.A. Khan, Shah Wali Ullah, Abdul Rahman Khan, Khalid Khan
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad

Data security has always been the most essential aspect of computing. Many users when connected on the cloud do not know that they could be victim of cybercrime. Cloud computing being a mega network spread globally, majority of cloud users mostly use it to benefit from the availability of mass storage. Due to increasing use of storage services, it is possible for malicious users to misuse cloud storage services. Cloud computing is flourishing at a greater speed and likewise security risks on cloud are also increasing day by day. A key challenge of cloud forensics is that the cloud service providers have not yet established forensic capabilities to support investigations in case of a digital compromise. Cloud Forensics has three dimensions: technical, organizational and legal. Technical Dimension includes tools required to perform forensic investigations, proactive measures, data collection, data labeling and evidence segregation. Evidentiary data collection in cloud environment is another main challenge as it is stored at providers and customers end. Organizational dimension is not only restricted to cloud providers and customers, but it widens when providers outsource their services to third parties. Legal dimension covers SLAs and jurisdiction issues to ensure data security. A critical evaluation of digital forensic investigations of cloud storage services is necessary to determine key challenges associated to this field. The focus of this study is to explore various digital forensic analysis approaches that facilitate speedy and authentic analysis of the incriminating activities happened on the cloud environment. In this study, we have evaluated different cloud forensics frameworks and techniques and have identified main key challenges related to cloud forensics. The study findings are reported herein.

Keywords: Cloud Computing, Digital Forensics, Cloud Forensics, Network Forensics, Forensics as a Service.

1. INTRODUCTION

Cloud computing provides wide ranging computational facilities at a cheaper cost to those organizations which cannot afford to setup data centers due to limited resources. The demand for cloud computing is increasing worldwide because of the popularity of digital devices and widespread use of the Internet. Cloud computing facilitates sharing of process units, storage devices and software. 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 (Damshenas, Dehghantanha, Mahmoud, and bin Shamsuddin, 2012)." Cloud computing is a virtualized platform of several host machines connected by the Internet. Despite its unmatched benefits, cloud computing can pose serious challenges for digital forensic analysis and cyber security investigations. The growing interest in cloud computing services presents opportunities for criminal exploitation and challenges for law enforcement agencies. For example, it is becoming easier for criminals to store incriminating files in the cloud computing environment, but it becomes almost impossible for law enforcing agencies to seize these files due to unavailability of information about the location of storage media. Hence, cloud computing makes computer forensic evidence acquisition and evidence analysis increasingly complex. The prominent challenges include difficulty in dealing with variety of data saved on different locations, restricted access to gather digital evidence on the cloud and inability to seize physical resources where digital assets have been compromised. Analyzing digital incidents in cloud environments is a difficult task since digital forensic methods used to perform ordinary digital investigations are not relevant to cloud computing environment (Simou, Kalloniatis, Mouratidis, and Gritzalis,

2015; Khan and Ullah, 2017).

1.1 An Overview of Digital Forensics

McKemmish (McKemmish, 1999) define digital forensic as the process of identifying, preserving, analyzing and presenting digital evidence in a way that is legally acceptable. The four elements in the Mckemmish (McKemmish, 1999) digital forensic model are the identification, preservation, analysis and presentation of digital evidence. Identification of the digital evidence pertains to its type, location and format (Khan and Wakeman, ; Rahman and Khan, 2015). Being part of the cyber infrastructure, the cloud computing paradigm is also prone to digital attacks. Cloud computing adds new challenges to forensic analysis as diversity of devices pose complexity issues. In the cloud paradigm, the identification of evidence is linked to identifying the cloud services used on the compromised devices. Preservation of the evidence means ensuring integrity of the evidential data acquired from the seized equipment (Khan, Chatwin, and Young, 2007b; Khan, 2012). In the analysis phase, the acquired digital evidence from the seized devices is transformed into a tangible sequence of activities in order to make it legally acceptable (Khan, Chatwin, and Young, 2007a). Both live and static analyses are conducted to transform the acquired evidentiary network data either from cache or storage devices (Bashir and Khan, 2013). The presentation phase relates to presenting digital evidence to the court of law. In the presentation phase, a comprehensible and scientifically proven methodology is required to be explained to the court to support authenticity of the acquired digital evidence (Rafique and Khan, 2013). A chain of custody genuinely starts when the evidentiary data is either seized or is preserved for analysis. To protect integrity of the acquired evidence, Department of the Premier and Cabinet, Western Australia suggests incorporating the following information in chain of custody:

—Person who acquired the evidence and who took possession of the evidence;
—The procedures used to collect the evidence;
—Artifacts from where the evidence was collected;
—Persons who accessed the acquired data with complete log of accessing the evidentiary data;
—The procedures adapted to store and protect the evidence and analyze it.

1.2 Cloud Forensic

Performing digital forensic analysis on the cloud poses a range of novel legal and technical challenges. Acquiring digital evidence from cloud computing platform is much more complex due to its distributed nature, elasticity data ownership and remote storage locations controlled by the service providers. An important consideration for selecting the right kind of approaches to acquire digital evidence in the cloud computing environment much depends on the type of cloud computing deployment model. The large volume of data available on the cloud poses a new challenge for forensic analysis. Determining geographical jurisdiction that pertains to digital evidence and capacity of law enforcing agencies to get access to the evidence when it is not available in their country is also another key challenge. The absence of guidelines to gather digital evidence in the cloud adds complexity to forensic analysis. In view of this there is a pressing need to put in place strong mechanism for forensic analysis in the cloud environment. Traces of evidence in the cloud computing environment are available on the servers, routers, switches etc. The process of conventional evidence collection methods in cloud computing environment is complicated due to technological constraints like distributed file systems, data stored on servers located at various jurisdictions, involvement of multiple stakeholders, proprietary and unstructured data formats. Another complexity of cloud computing is linked to the fact that some organizations prefer to encrypt data before storing it on the cloud. In the event of a digital crime, determining true nature of the compromised data may be difficult to predict due to encryption. Interestingly, the Information Commissioners Office in UK released an advice in 2010 for the cloud users to encrypt their data particularly the personal and sensitive data prior to transferring it to the cloud. The current digital forensics methods do not fit-for-purpose for cloud computing environment. From

digital forensic analysis perspective, the evidence acquisitions and analysis in cloud computing is much more complex than the ordinary monolithic systems. Computer forensics serves as an important tool to curb the digital crimes. But in the cloud computing, migrated data only represents a snapshot of actual data stored on the cloud. On public cloud, the service providers can record information about cloud usage by the users. Such information relates to the use of services, for instance, Google logs Google Docs usage information in the form of storage usage, login details, IP address through which the services were accessed along with date and time of access. The information recorded by the service provider may retain for a long time even if the user had deleted his/her files. In case the cloud service provider agrees to provide access to this information, then it can facilitate digital forensic analysis. However, one importance strength of cloud computing is that evidence on it cannot be easily destroyed by the criminals as it may be mirrored on multiple devices. Aggregating of logs from clients and servers can provide meticulous details of suspicious activity happened on the cloud-based systems (Khan and Ullah, 2017). Digital forensics and incident response have been critical parts of digital investigations and these tasks have become more challenging with the rapid evolution of cloud.

2. LITERATURE REVIEW

Martini and Choo (Martini and Choo, 2012) highlight digital forensic investigation related challenges that have emerged due to increased use of cloud computing in the business sector. The study proposes an integrated and interactive framework based on two contemporary digital forensic investigation frameworks namely NIST and McKemmish (Martini and Choo, 2012) . The aim of the study was to propose a powerful and efficient digital forensic framework to be used in the cloud environment by combining different phases of the existing frameworks. The amalgamation of approaches used for different phases of the forensic analysis process could be more effective to produce better analysis. The significance of study is to fuse different phases of digital forensic analysis frameworks to achieve better results. Taylor et al. (Taylor, Haggerty, Gresty, and Hegarty, 2010) address the problem of volatility of evidentiary data on the cloud. Since, a cloud environment is a virtual environment, so all types of evidentiary data maintained by the operating system such as information pertaining to the launch/execution of application programs, temporary internet files, logs and registry entries are lost when the user closes the sessions. This caveat results in a serious difficulty to recover data from the hard disks. Given these constraints, study explores legal aspects of digital forensic analysis within the realms of cloud computing. Dykstra and Sherman (Dykstra and Sherman, 2012) investigate technicalities and trust issues related to collection of acquiring digital evidence from infrastructure-as-a-service platform. The authors address core issue of acquiring evidentiary data and analyze certain tactics to tackle these issues and challenges. The study aims at evaluating various digital acquisition tools to develop more suitable and forensically sound data acquisition approaches to assist law enforcement agencies and forensic examiners to acquire trustworthy digital evidence from the cloud. Data acquisition in cloud can only be done in one of two ways: either examiner remotely collects data through privileged access provided by the CSP or data is supplied to the examiners by the CSP. In both the cases, the degree of trust related to the acquired data still remains a big question mark. Yan (ChengYan, 2011) focuses on security issues related to the cloud services. To thwart cybercrimes, the authors proposed a cloud forensic framework by defining an analysis engine as a network service that monitors the network to find an anomalous behavior and starts collecting evidence in case the analysis engine indicates towards the happening of a digital incident. The collected evidence is then analyzed using famous forensic analysis tools like Encase and FTK. The aim of study was to present a vibrant framework to thwart cybercrime by observing suspicious behaviors over the network. Cloud computing provides lesser support to forensic examiners to perform forensic investigations. Given this problem, the study in (Dykstra and Sherman, 2013) proposes design and implementation of a forensic analysis tool called FROST (Forensic OpenStack Tools). FROST is a collection of three forensic analysis tools especially designed for

cloud platform. The proposed implementation of the OpenStack tool is based on IaaS (infrastructure as a Service) platform. The proposed set of forensic analysis tools supports collection of trustworthy evidence from firewall, API logs and virtual disks. The aim of study was to provide tool support based on theoretical foundation. The study in (Taylor, Haggerty, Gresty, and Lamb, 2011) addresses security threats linked to cloud computing environment accessed through Internet. Though regional storage options are being provided by the cloud providers, but there is always a chance that data is replicated on multiple sources. The study classifies computers and technology crimes in three different ways. But, the analytical paradigm is less effective on cloud computing as it is spread over users, applications, data, and servers. The study states that computer forensics follow a linear process through which it identifies extracts, analyzes and presents digital evidence. The study in (Chung, Park, Lee, and Kang, 2012) proposes a procedure for examining and analyzing all the devices that are used to access cloud artifacts such as Android smartphone, iPhone, Mac and Windows systems. The proposed solution addresses forensic analysis of cloud storage services which is a kind of IaaS. Cloud users utilize cloud storage to save documents, emails and multi-media stuff. To handle these types of different documents and multi-media stuff, the cloud storage is also used to store various types of applications. The study in (Ruan, Carthy, Kechadi, and Baggili, 2013) is based on the survey results conducted from experts and practitioners of digital forensics. The survey questionnaire was based on the issues related to cloud computing forensics. The survey questions basically addressed the definition, challenges, scope, missing capabilities and opportunities related to the cloud computing forensics. The survey participants were not only experienced but also had fair knowledge of digital forensics. The aim of the study was to recommend a suitable mechanism to address fundamental issues in the domain of cloud computing forensics. The digital evidence available on the cloud could be in the form of virtual machine images, logs provided by the CSP, files stored on the cloud storage and traces of file system activities on the cloud metadata files. Cloud forensics becomes extremely difficult due to lack of investigator's control over the cloud. Investigators remain dependent on CSP for provision of logs and have to blindly trust integrity of information provided by the CSP. Also, in case the virtual machine is shut down then there is no mechanism to access these logs. The objective of the study in (Zawoad, Dutta, and Hasan, 2013) is to propose a mechanism to securely acquire logs from the virtual machines. The proposed solution is named as Secure-Logging-as-a-Service (SecLaaS). The analysis of different types of logs such as network logs and process logs etc. can reveal useful information. But the problem of acquiring logs on the cloud platform itself is a gigantic task due to multi-tenant cloud models and black-box nature of the cloud. Sang (Sang, 2013) addresses the challenge of identification of evidence in cloud computing. The study focuses on forecasting challenges of applying computer forensics on three service models i.e. IaaS, PaaS, and SaaS. The authors consider logging of illegal activities on the cloud as a viable approach for implementing digital forensics on the cloud relatively with ease. Pasquale et al. (Pasquale, Hanvey, Mcgloin, and Nuseibeh, 2016) used attack scenarios for configuration of more effective evidence collection on the cloud. The evidence collection techniques are designed to detect possible attack scenarios violating the security policies. The study explains various attack and evidence collection scenarios while also illustrating the examples of inside and outside attacks. The results show that various attack scenarios help to target evidence collection through security breaches while saving space, and time necessary to store and process data. Pichan et al. (Pichan, Lazarescu, and Soh, 2015) provide a systematic survey of challenges related to digital forensic analysis in cloud computing paradigm. The study also discusses the recent developments and the latest trends and solutions proposed for cloud forensics. The aim of study was to discover various cloud forensics process models along with their challenges and proposed solutions. Federici (Federici, 2014) highlights problem behind the availability of cloud storage at cheaper cost. As user gets it mostly for free, there is a greater chance of criminal activity being taken place. The study describes the concept and internals of Cloud Data Image Library, the middle layer accessing read-only data files and folders for supporting technologies

like Dropbox, Google drive and Microsoft storage drive. There is a wide concern over stored data being accessed by the cloud providers. The paper leverages cloud providers with access over the data being stored over cloud and makes users vulnerable to be hijacked by them. Hale (Hale, 2013) reviews a scenario of cloud storage using Amazon Cloud Drive. It discusses the artifacts left behind after Amazon Cloud Drive is used to access or upload files. The study examines Amazon Cloud Drive to retrieve the artifacts from an unallocated space over the Cloud Drive. The study highlights various procedures to gather file transfers information to and from cloud drive. Quick and Choo (Quick and Choo, 2014) addresses emerging challenges that have evolved with cloud storage. Getting digital evidence from cloud storage services remains a challenge due to virtualization, lack of knowledge of tracing the location of evidence, privacy issues and legal boundaries. In this study, Google Drive is taken as a case study and identification of artifact that remains after use of drive storage were made through experimentation on desktop and iPhone3G platform. The various functional components of the cloud and the areas where forensics solutions proposed in the reviewed contemporary studies are shown in Figure 1.

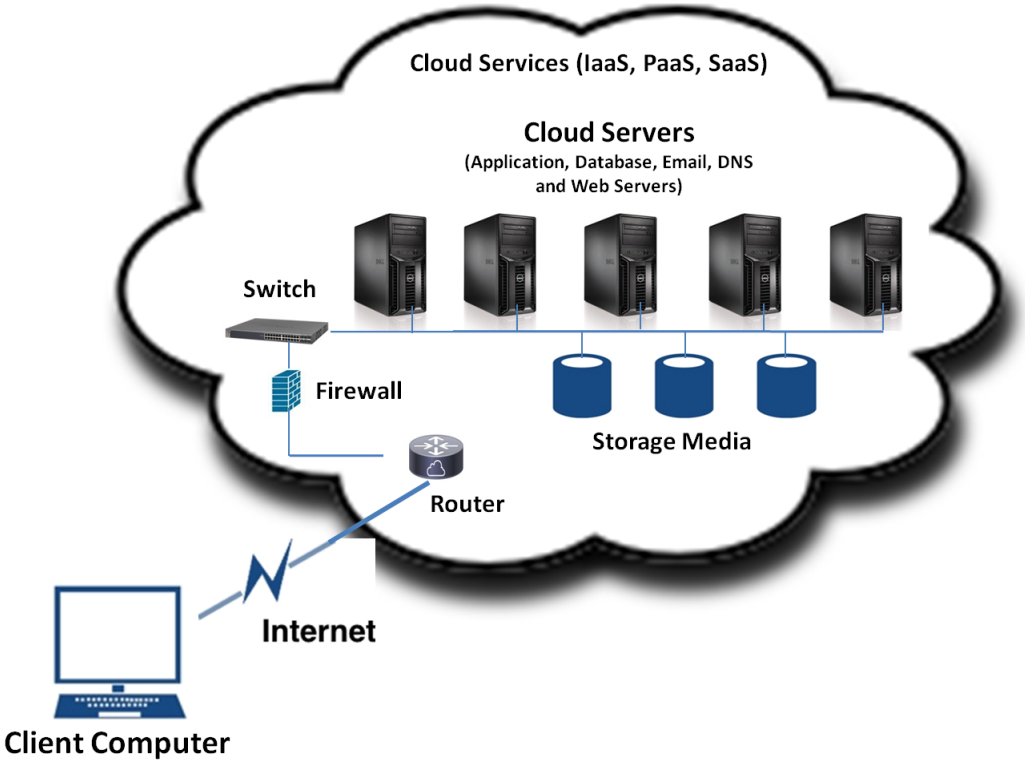

Figure 1. Functional components of the cloud for potential forensics investigations.

2.1 Critical Analysis

The main objective of our study is to explore the existing digital forensic analysis techniques in the domain of cloud computing. Another objective is to critically evaluate strengths and weakness of the current forensic analysis technique being employed in the area of cloud computing. The review is restricted to analyzing approaches for digital evidence collection, evidence preservation, storage forensics, log analysis and timeline generation techniques. The critical analysis will help determine the key challenges linked to this domain. A critical analysis of the various data acquisition, preservation and analysis techniques for the cloud environment as discussed in the previous section is provided below.

Ref No.	Focused Area	Scope	Approach	Data Sources	Content Analyzed	Assumptions for evidence collection	Dependency on CSP?	Applicability - Cloud Models (Platform)	Applicability - Type of Cloud	Validation Parameters
(Martini and Choo, 2012)	Integrated and interactive forensic framework	Evidence collection and preservation	iterative	Client Devices, Virtual Machines	Logs	VMs are not destroyed when user exits	High	Private, public and hybrid	SaaS IaaS PaaS	Data Integrity, Performance
(Taylor et al., 2010)	Handling volatility of evidentiary data on cloud	Evidence Collection	Acquire required data from CSP	repositories, cache memory	Images, documents, emails	Requesting CSP through subpoena	High	Public	SaaS	Data Integrity
(Dykstra and Sherman, 2012)	Trust issues related to acquiring digital evidence	Evidence Collection	Acquire required data from CSP	Virtual Machines	Logs	Forensics as a Service	High	Public	IaaS	Data Integrity
(ChengYan, 2011)	Thwart cybercrimes by monitoring network	Network monitoring	Automatic data collection and through CSP	Various artifacts in a data centre facility	Logs, emails and digital signatures	Network Forensic Service is available	High	Private and Public	IaaS PaaS SaaS	Data Integrity, Performance, Scalability
(Dykstra and Sherman, 2013)	Implementation forensic analysis tool called FROST	Collection of digital evidence	Acquire required data from CSP	Virtual disks	Firewall and API logs	Trusting host OS, and networks infrastructure	High	Public	IaaS	Data Integrity (checksums)
(Taylor et al., 2011)	Security threats to cloud computing environment	Collecting, evidence	Exploring local devices	Client Devices, VM, Servers	All types of logs	Cloud providers can provide VM location	High	Public Private Hybrid	IaaS PaaS SaaS	Data Integrity
(Chung et al., 2012)	Procedure for analyzing devices used to access the cloud artifacts	Examining traces of cloud storage on users devices	Exploring local devices	PC terminals, PDAs and Smartphones	Documents, emails and video clips	Downloaded files on local devices are not deleted	None	Public Private Hybrid	IaaS	Data Integrity
(Ruan et al., 2013)	Addressing fundamental issues in the domain of cloud forensics	Developing procedures to enhance forensic capabilities	Survey based study	Local devices and Virtual Machines	Any	Based on opinions of the survey participants	-	Public Private Hybrid	IaaS PaaS SaaS	-
(Zawoad et al., 2013)	Secure-Logging-as-a-Service to reduce dependence on CSP	Evidence Collection	Make SLAs to bound CSP to ensure logs integrity	Virtual Machines	Logs	CSP is legally bound to provide logs	High	Public	IaaS PaaS SaaS	Data Integrity
(Sang, 2013)	Identification of evidence in cloud computing	Evidence Collection	Additional logging at server side	VM	Logs	Ensure logging mechanism at CSP side	Low	Public	IaaS PaaS SaaS	Data Integrity
(Pasquale et al., 2016)	Secure evidence collection in cloud	Evidence Collection	-	Local devices and VMs	Logs	-	High	Public	PaaS	Data Integrity
(Pichan et al., 2015)	Challenges linked to cloud forensics	Evidence Collection	DFaaS	VMs, Servers	Logs	Deploying DFaaS on CSP side	High	Public	SaaS	Data Integrity
(Federici, 2014)	Proactive forensic techniques to secure cloud storage devices	Averting cybercrimes	Mitigating cloud attacks	VM, Servers	Logs	Monitoring all types of logs to identify malicious activity	High	Public	IaaS PaaS SaaS	Data Integrity
(Hale, 2013)	Analyzing Amazon Cloud Drive to retrieve artifacts from unallocated space	Perl scripts to retrieve evidence from Cloud Drive	Monitoring user accesses on Cloud Drive	Storage drives	Logs, file system activity, network packets	Monitoring how cloud drives are accessed	High	Public	IaaS PaaS SaaS	Data Integrity
(Quick and Choo, 2014)	Addressing challenges that have evolved with cloud storage	Acquiring evidence from cloud storage	Artifact that remains after use of cloud storage	Google Drive, PCs, Smartphone	Logs	-	High	Public	IaaS PaaS SaaS	Data Integrity

Table I: Event details sent by the baseline agent to the server-side listener

3. KEY CHALLENGES CLOUD FORENSICS

Evidence collection from cloud poses a great challenge due to limited access of clients on the cloud infrastructure and involvement of CSP in the acquisition process. The prominent key challenges pertaining to cloud forensics are listed below.

—The most prominent challenge for cloud forensics is that potential evidence resides on scattered places all over the world in a virtualized environment.

—Employing unique procedure for cloud forensics is not possible in the cloud. Different forensics techniques are required to be used depending on the cloud deployment and service model. In other words, different approaches are required to investigate IaaS, PaaS and SaaS service models as well as Private and Public clouds due to their atypical structure.

—Particularly in the public cloud deployment model, consumers do not have physical access to the infrastructure and privacy of their data is far less than the ones in the private cloud.

—If there are no provisions in the SLAs to provide evidentiary logs to the clients, then CSP can simply refuse to provide such data. Even if CSP agrees to provide evidentiary data, then there still remains a question whether the CSP has provided complete logs data or certain parts of logs are scrubbed.

—Client computers in the cloud environment may provide minimal evidence due to storage of actual data on the CSP side. Hence, triages on the client side can never be authentic.

—Specialized tools are needed to determine if any residual artifacts remain on the devices when these devices interact with cloud services.

—here is a lack of guidelines, methods, best practices and tools to extract evidence in a forensically sound manner.

—Legal issues concerning jurisdiction of physical devices in the cloud, data retention and privacy laws need to be revisited and duly accounted for in the SLAs.

—The timestamp matching of different file system activities during the investigation can be complicated since client and cloud storage server may reside in different time zones.

—Physical seizure of computer devices containing potential evidence is virtually not possible in the cloud environment. This aspect severely hinders the forensic investigative process and raises serious questions about the authenticity of investigation.

—Issues related to jurisdiction, multi-tenancy and dependence on CSPs make forensic investigation even more complex.

—Virtual machines are used in the cloud and all the data is lost when virtual machine is rebooted or turned off. In this way, the evidentiary evidence such as executing processes, registry entries, temporary Internet files and memory content are lost.

4. CONCLUSION AND FUTURE WORK

This study evaluated the efficacy and effectiveness of various approaches which have been proposed in the contemporary literature related to the forensic analysis of storage devices over the cloud. The outcome of this study is in the form of a critical analysis warranting merits and demerits of the existing digital forensic approaches being employed in the domain of cloud. It is envisaged that review of these approaches will be beneficial to understand the existing research gaps and explore potential future work in this area.

References

Bashir, M. S. and Khan, M. 2013. Triage in live digital forensic analysis. *International journal of Forensic Computer Science 1*, 35–44.

ChengYan. 2011. Cybercrime forensic system in cloud computing. In *2011 International Conference on Image Analysis and Signal Processing*. 612–615.

Chung, H., Park, J., Lee, S., and Kang, C. 2012. Digital forensic investigation of cloud storage services. *Digital investigation 9,* 2, 81–95.

Damshenas, M., Dehghantanha, A., Mahmoud, R., and bin Shamsuddin, S. 2012. Forensics investigation challenges in cloud computing environments. In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. 190–194.

Dykstra, J. and Sherman, A. T. 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation 9*, S90–S98.

Dykstra, J. and Sherman, A. T. 2013. Design and implementation of frost: Digital forensic tools for the openstack cloud computing platform. *Digital Investigation 10*, S87–S95.

Federici, C. 2014. Cloud data imager: A unified answer to remote acquisition of cloud storage areas. *Digital Investigation 11,* 1, 30–42.

Hale, J. S. 2013. Amazon cloud drive forensic analysis. *Digital Investigation 10,* 3, 259–265.

Khan, M., Chatwin, C. R., and Young, R. C. 2007a. A framework for post-event timeline reconstruction using neural networks. *digital investigation 4,* 3-4, 146–157.

Khan, M. and Wakeman, I. Machine learning for post-event timeline reconstruction. Citeseer.

Khan, M. N. A. 2012. Performance analysis of bayesian networks and neural networks in classification of file system activities. *Computers & Security 31,* 4, 391–401.

Khan, M. N. A., Chatwin, C. R., and Young, R. 2007b. Extracting evidence from filesystem activity using bayesian networks. *International journal of Forensic computer science 1*, 50–63.

Khan, M. N. A. and Ullah, S. 2017. A log aggregation forensic analysis framework for cloud computing environments. *Computer Fraud & Security 2017,* 7, 11–16.

Martini, B. and Choo, K.-K. R. 2012. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation 9,* 2, 71 – 80.

McKemmish, R. 1999. *What is forensic computing?*

Pasquale, L., Hanvey, S., Mcgloin, M., and Nuseibeh, B. 2016. Adaptive evidence collection in the cloud using attack scenarios. *Computers & Security 59*, 236–254.

Pichan, A., Lazarescu, M., and Soh, S. T. 2015. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation 13*, 38–57.

Quick, D. and Choo, K.-K. R. 2014. Google drive: forensic analysis of data remnants. *Journal of Network and Computer Applications 40*, 179–193.

Rafique, M. and Khan, M. 2013. Exploring static and live digital forensics: Methods, practices and tools. *International Journal of Scientific & Engineering Research 4,* 10, 1048–1056.

Rahman, S. and Khan, M. 2015. Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology 8,* 2, 379–88.

Ruan, K., Carthy, J., Kechadi, T., and Baggili, I. 2013. Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. *Digital Investigation 10,* 1, 34–43.

Sang, T. 2013. A log based approach to make digital forensics easier on cloud computing. In *2013 Third International Conference on Intelligent System Design and Engineering Applications*. 91–94.

Simou, S., Kalloniatis, C., Mouratidis, H., and Gritzalis, S. 2015. Towards the development of a cloud forensics methodology: a conceptual model. In *International Conference on Advanced Information Systems Engineering*. Springer, 470–481.

Taylor, M., Haggerty, J., Gresty, D., and Hegarty, R. 2010. Digital evidence in cloud computing systems. *Computer law & security review 26,* 3, 304–308.

Taylor, M., Haggerty, J., Gresty, D., and Lamb, D. 2011. Forensic investigation of cloud computing systems. *Network Security 2011,* 3, 4 – 10.

Zawoad, S., Dutta, A. K., and Hasan, R. 2013. Seclaas: secure logging-as-a-service for cloud forensics. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM, 219–230.

M.N.A. Khan obtained a D.Phil. degree in computer system engineering from the University of Sussex, UK. His research interests are in the fields of software engineering, cyber administration, digital forensic analysis and machine learning techniques.

Shah Wali Ullah obtained an MS degree in computer science from Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad. His research interests are in the fields of digital forensics and software engineering.

Abdul Rahman Khan obtained his MS(MS) degree from Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad. He has worked on various Research and Development projects. His research interests include finance, quality control management, technical management, project planning and cyber administration.

Khalid Khan obtained his MS(SE) degree from Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad. His research interests include software engineering, digital forensics and cloud computing.